AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of North Carolina, Western Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
5:23-CV-570-D-RJ	10/11/2023	Eastern District of North Carolina, Western Division

PLAINTIFF	DEFENDANT
Telefonaktiebolaget LM Ericsson et al.	Lenovo (United States), Inc. et al.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,151,430	12/19/2006	Telefonaktiebolaget LM Ericsson
2	9,509,273	11/29/2016	Telefonaktiebolaget LM Ericsson
3	9,313,178	4/12/2016	Ericsson AB
4	11,122,313	9/14/2021	Ericsson AB
5	10,972,654	4/6/2021	Telefonaktiebolaget LM Ericsson

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Peter A. Moore, Jr.	Stephanie Mann	10/12/2023

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Google Exhibit 1002
Google v. Ericsson

Trials@uspto.gov
Tel: 571-272-7822

Paper 17
Date: December 30, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner.

IPR2022-00618
Patent 9,313,178 B2

Before GEORGIANNA W. BRADEN, NATHAN A. ENGELS, and NORMAN H. BEAMER, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

TERMINATION
Due to Settlement After Institution of Trial
Granting Joint Request to Treat Settlement
Agreement as Business Confidential Information
35 U.S.C. § 317; 37 C.F.R. § 42.74

I. INTRODUCTION

Apple Inc. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–20 of U.S. Patent No. 9,313,178 B2 (Exhibit 1001, "the '178 patent") under 35 U.S.C. §§ 311–319. Paper 2. Telefonaktiebolaget LM Ericsson ("Patent Owner") filed a Preliminary Response. Paper 9.

On September 1, 2022, the Board instituted an *inter partes* review of claims 1–20 of the '178 patent. Paper 11.

On December 16, 2022, after receiving Board authorization, Petitioner and Patent Owner filed a Joint Motion to Terminate Proceeding under 35 U.S.C. § 317(a) and 37 C.F.R. § 42.74. Paper 15. As Exhibit 1016, the parties filed a copy of an agreement titled "Global Patent License Agreement." Ex. 1016, 1. The parties also filed a Joint Request to Treat Settlement Agreement as Business Confidential Information under 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74(c). Paper 16.

II. DISCUSSION

The parties represent that they "have reached a settlement as to all the disputes in this proceeding and as to the '178 patent." Paper 15, 2. The parties represent that a "true copy of the settlement agreement" is filed as Exhibit 1016. *Id.* The parties also represent that "[n]o other such agreements, written or oral, exist between or among" the parties. *Id.*

The parties assert that termination "would save significant further expenditure of resources by" the parties. Paper 15, 2. The parties assert that termination "would also further the purpose of *inter partes* review proceedings, which seek to provide an efficient and less costly alternative forum for patent disputes." *Id.* at 2–3. Additionally, the parties contend that

"maintaining the proceeding would discourage further settlements, as patent owners in similar situations would have a strong disincentive to settle if they perceived that an *inter partes* review would continue regardless of a settlement." *Id.* at 3.

This proceeding has not progressed very far. Patent Owner has not filed its Response. Terminating this proceeding will save the Board administrative and judicial resources, e.g., in conducting an oral argument and issuing a final written decision to decide the patentability issues raised in the Petition. Further, "[t]here are strong public policy reasons to favor settlement between the parties to a proceeding," and "[t]he Board expects that a proceeding will terminate after the filing of a settlement agreement, unless the Board has already decided the merits of the proceeding." Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,768 (Aug. 14, 2012).

Under these circumstances, we determine that it is appropriate to terminate this proceeding. We also determine that it is appropriate to treat the parties' settlement agreement (Exhibit 1016) as business confidential information under 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74(c).

This Order does not constitute a final written decision under 35 U.S.C. § 318(a).

III. ORDER

Accordingly, it is

ORDERED that the parties' Joint Motion to Terminate Proceeding (Paper 15) is granted;

FURTHER ORDERED that this proceeding is terminated as to all parties; and

FURTHER ORDERED that the parties' Joint Request to Treat Settlement Agreement as Business Confidential Information (Paper 16) is granted, and the parties' settlement agreement (Exhibit 1016) shall be treated as business confidential information and be kept separate from the file of U.S. Patent No. 9,313,178 B2 and made available only under the provisions of 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74(c).

For PETITIONER:

W. Karl Renner
Thomas Rozylowicz
Nicholas Stephens
FISH & RICHARDSON P.C.
axf-ptab@fr.com
tar@fr.com
nstephens@fr.com

For PATENT OWNER:

Peter C. Knops
Jason Wejnert
NOROOZI PC
peter@noroozipc.com
jason@noroozipc.com

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00001	1/8/2021	for the Eastern District of Texas

PLAINTIFF	DEFENDANT
ERICSSON INC., TELEFONAKTIEBOLAGET LM ERICSSON, AND ERICSSON AB	SAMSUNG ELECTRONICS CO., LTD., AND SAMSUNG ELECTRONICS AMERICA, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,151,430	12/19/2006	TELEFONAKTIEBOLAGET LM ERICSSON
2	6,879,849	4/12/2005	TELEFONAKTIEBOLAGET LM ERICSSON
3	7,286,823	10/23/2007	TELEFONAKTIEBOLAGET LM ERICSSON
4	9,313,178	4/12/2016	ERICSSON AB
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

ORDERED that all of Ericsson's patent infringement claims and all of Samsung's patent infringement counterclaims are DISMISSED WITH PREJUDICE

CLERK	(BY) DEPUTY CLERK	DATE
David A. O'Toole	ch	6/2/21

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00001	1/8/2021	for the Eastern District of Texas

PLAINTIFF	DEFENDANT
ERICSSON INC., TELEFONAKTIEBOLAGET LM ERICSSON, AND ERICSSON AB	SAMSUNG ELECTRONICS CO., LTD., AND SAMSUNG ELECTRONICS AMERICA, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,151,430	12/19/2006	TELEFONAKTIEBOLAGET LM ERICSSON
2 6,879,849	4/12/2005	TELEFONAKTIEBOLAGET LM ERICSSON
3 7,286,823	10/23/2007	TELEFONAKTIEBOLAGET LM ERICSSON
4 9,313,178	4/12/2016	ERICSSON AB
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,313,178 B2
APPLICATION NO. : 14/266368
DATED : April 12, 2016
INVENTOR(S) : Ma et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page

In Item (56), under "OTHER PUBLICATIONS", in Column 2, Line 7, delete "-BE9E000D8435/" and insert -- -BE9E0C0D8435/ --, therefor.

In the Specification

In Column 4, Lines 4-27, delete "In one embodiment.....format header." and insert the same at Line 3, after "key.", as a continuation paragraph.

In Column 5, Lines 26-52, delete "The transcoded content is then.....data centers." and insert the same at Line 25, after "resolutions.", as a continuation paragraph.

In Column 5, Line 46, delete "manger" and insert -- manager --, therefor.

In Column 7, Lines 45-63, delete "In one embodiment..... previous key." and insert the same at Line 46, as a new paragraph.

Signed and Sealed this
Tenth Day of October, 2017

Joseph Matal

Joseph Matal
Performing the Functions and Duties of the
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,313,178 B2

APPLICATION NO. : 14/266,368

ISSUE DATE : April 12, 2016

INVENTOR(S) : Ma, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Face Page, in Field (56), under "OTHER PUBLICATIONS", in Column 2, Line 7, delete "-BE9E000D8435/" and insert - - -BE9E0C0D8435/ - -, therefor.

In Column 4, Lines 4-27, delete "In one embodiment……format header." and insert the same at Line 3, after "key.", as a continuation paragraph.

In Column 5, Lines 26-52, delete "The transcoded content is then ……data centers." and insert the same at Line 25, after "resolutions.", as a continuation paragraph.

In Column 5, Line 46, delete "manger" and insert - - manager - -, therefor.

In Column 7, Lines 45-63, delete "In one embodiment…… previous key." and insert the same at Line 46, as a new paragraph.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

6300 Legacy, MS EVR 1-C-11
Plano, TX 75024
972-583-8656

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14266368
Filing Date:	30-Apr-2014
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Filer:	Steven Ware Smith/Kara Coffman
Attorney Docket Number:	P43758-US3

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Certificate of Correction	1811	1	100	100

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**100**

Electronic Acknowledgement Receipt	
EFS ID:	26183754
Application Number:	14266368
International Application Number:	
Confirmation Number:	9269
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Customer Number:	27045
Filer:	Steven Ware Smith/Kara Coffman
Filer Authorized By:	Steven Ware Smith
Attorney Docket Number:	P43758-US3
Receipt Date:	27-JUN-2016
Filing Date:	30-APR-2014
Time Stamp:	15:32:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$100
RAM confirmation Number	2018
Deposit Account	501379
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	P43758-US3_2016-06-27_CoC_Request_Letter.pdf	92237 9f0839ea2394a6a5730851ee7d7b419a9b4ce018	no	3
Warnings:					
Information:					
2	Request for Certificate of Correction	P43758-US3_2016-06-27_CoC_PTO-1050.pdf	123405 fd89a0ff5ce9ce2e9706c23f1a3463b73b7584cf	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30475 8dfdad7f7ac275626542c21c2ecdd405e32af63a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	246117		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF: U.S. Patent No. 9,313,178

USPTO CONFIRMATION CODE: 9269

APPLICATION NO.: 14/266,368

FILED: April 30, 2014

EXAMINER: Brandon Hoffman

GROUP ART UNIT: 2433

FOR: METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

37 CFR 1.322 & 37 CFR 1.323 REQUEST FOR CERTIFICATE OF CORRECTION FOR USPTO AND/OR APPLICANT MISTAKE

HONORABLE COMMISSIONER OF PATENTS & TRADEMARKS

SIR:

The following is a request for a certificate of correction in Serial Number 14/266,368, now Patent Number 9,313,178.

A certificate of correction under 35 USC 254 is respectfully requested in the above-identified patent.

The errors were the fault of both the applicant and USPTO and, accordingly, please charge **$100.00** to our Deposit Account No. 50-1379. In the event that a further fee is required, please charge the amount to the same Deposit Account.

The exact locations where the errors appear in the patent and patent application are as follows:

On the Face Page, in Field (56), under “OTHER PUBLICATIONS”, in Column 2, Line 7, delete “-BE9E000D8435/” and insert - - -BE9E0C0D8435/ - -, therefor.
(LIST OF REFERENCES CITED BY APPLICANT AND CONSIDERED BY EXAMINER DATED MAY 26, 2015, SHEET 2 (PAGE 56 OF FW), UNDER “NON-PATENT LITERATURE DOCUMENTS”, ENTRY 2, LINE 2)

In Column 4, Lines 4-27, delete “In one embodiment……format header.” and insert the same at Line 3, after “key.”, as a continuation paragraph.
(ORIGINALLY FILED SPECIFICATION DATED APRIL 30, 2014, PAGE 5, LINES 6-20)

In Column 5, Lines 26-52, delete “The transcoded content is then ……data centers.” and insert the same at Line 25, after “resolutions.”, as a continuation paragraph.
(ORIGINALLY FILED SPECIFICATION DATED APRIL 30, 2014, PAGE 7, LINES 6-22)

In Column 5, Line 46, delete “manger” and insert - - manager - -, therefor.
(ORIGINALLY FILED SPECIFICATION DATED APRIL 30, 2014, PAGE 7, LINE 19)

In Column 7, Lines 45-63, delete “In one embodiment…… previous key.” and insert the same at Line 46, as a new paragraph.
(ORIGINALLY FILED SPECIFICATION DATED APRIL 30, 2014, PAGE 10, LINES 15-26)

The requested corrections are attached on Form PTO 1050.

Respectfully Submitted

, 2016

DATE

/Ronald J. Ward,Reg#54870/

Ronald J. Ward
Registration No. 54,870
Attorney of Record

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/266,368	04/12/2016	9313178	P43758-US3	9269

27045 7590 03/23/2016
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Kevin J. Ma, Nashua, NH;
Ericsson AB, Stockholm, SWEDEN;
Robert Hickey, Bedford, MA;
Paul Tweedale, Andover, MA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27945 3500 10/28/2015

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/266,368	04/30/2014	Kevin J. Ma	P43758-US3	9269

TITLE OF INVENTION: METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

APPLN TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/28/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOFFMAN, BRANDON S	2433	713-168000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1.

2.

3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

ERICSSON AB

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

STOCKHOLM, SWEDEN

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies .....

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 50-1379 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature / Ronald S. Liu, Reg. No. 64,170 / Date January 28, 2016

Typed or printed name Ronald S. Liu Registration No. 64,170

Electronic Patent Application Fee Transmittal

Application Number:	14266368
Filing Date:	30-Apr-2014
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Filer:	Steven Ware Smith/Kathryn Lopez
Attorney Docket Number:	P43758-US3

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**960**

Electronic Acknowledgement Receipt	
EFS ID:	24750359
Application Number:	14266368
International Application Number:	
Confirmation Number:	9269
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Customer Number:	27045
Filer:	Steven Ware Smith/Kathryn Lopez
Filer Authorized By:	Steven Ware Smith
Attorney Docket Number:	P43758-US3
Receipt Date:	28-JAN-2016
Filing Date:	30-APR-2014
Time Stamp:	13:04:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$960
RAM confirmation Number	16328
Deposit Account	501379
Authorized User	LIU, RONALD S.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P43758-US3_2016-01-28_16-3516_Issue_Fee_Transmittal.pdf	304894 775d6efe73a218e620778ca9e416d0644f2125b4	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30823 0fe6c055d8b77582fd7d2404448497f522dce771	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	335717		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

27045 7590 10/28/2015
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2433	

DATE MAILED: 10/28/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/266,368	04/30/2014	Kevin J. Ma	P43758-US3	9269

TITLE OF INVENTION: METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/28/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27045 7590 10/28/2015
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/266,368	04/30/2014	Kevin J. Ma	P43758-US3	9269

TITLE OF INVENTION: METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	01/28/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOFFMAN, BRANDON S	2433	713-168000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/266,368	04/30/2014	Kevin J. Ma	P43758-US3	9269

27045 7590 10/28/2015
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2433	

DATE MAILED: 10/28/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/266,368	Applicant(s) MA ET AL.	
	Examiner BRANDON HOFFMAN	Art Unit 2433	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed August 26, 2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-20*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/BRANDON HOFFMAN/
Primary Examiner, Art Unit 2433

1. The present application is being examined under the pre-AIA first to invent provisions.

REASONS FOR ALLOWANCE

2. The following is an examiner's statement of reasons for allowance: the prior art of record (Kamath 20050060316) does not teach detecting content key rotation boundaries and issuing requests to a license server ahead of the key rotation boundaries.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRANDON HOFFMAN/
Primary Examiner, Art Unit 2433

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
713	168 - with keyword limiters	5-12-15	BH

SEARCH NOTES

Search Notes	Date	Examiner
inventor name search	5-12-15	BH
see attached EAST search notes	5-12-15	BH
updated EAST search notes	10-20-15	BH

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	searched claim language	10-20-15	BH

	/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

CPC						
Symbol					**Type**	**Version**
H04L		63	/	0428	F	2013-01-01
H04L		9	/	0891	I	2013-01-01
H04L		2209	/	60	A	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433 (Primary Examiner)	10/20/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

U.S. Patent and Trademark Office

Part of Paper No. 20151020

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
713	168	H	0	4	L	9 / 32 (2006.01.01)	H	0	4	L	9 / 32 (2006.01.01)

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433 (Primary Examiner)	10/20/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

U.S. Patent and Trademark Office

Part of Paper No. 20151020

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☐ **T.D.** ☐ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433 (Primary Examiner)	10/20/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

U.S. Patent and Trademark Office

Part of Paper No. 20151020

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	169950	playback	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L2	78178	encryption near key	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L3	11487	key near identifier	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L4	159719	expiration	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L5	194766	manifest	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L6	3618	license near server	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L7	9006	key near rotation	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L8	3	L1 and L2 and L3 and L4 and L5 and L6 and L7	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L14	201554	key.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L15	135224	serial$3.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L16	12773	license.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L17	54707	expir$5.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20
L18	48	L14 and L15 and L16 and L17	US-PGPUB; USPAT; USOCR	OR	ON	2015/10/20 15:20

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	2063	encrypt$3 with expir$5	USPAT; * No UPAD	OR	ON	2015/10/20 15:20
L10	4440	license with server	USPAT; * No UPAD	OR	ON	2015/10/20 15:20
L11	8779	key near rotat$4	USPAT; * No UPAD	OR	ON	2015/10/20 15:20
L12	205	L9 and L10	USPAT; * No UPAD	OR	ON	2015/10/20 15:20
L13	2	L11 and L12	USPAT; * No UPAD	OR	ON	2015/10/20 15:20

10/20/2015 3:21:07 PM
C:\Users\bhoffman\Documents\EAST\Workspaces\14266368.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/12/2015	10/20/2015							
	1	=	=							
	2	=	=							
	3	=	=							
	4	=	=							
	5	=	=							
	6	=	=							
	7	=	=							
	8	=	=							
	9	=	=							
	10	=	=							
	11	=	=							
	12	=	=							
	13	=	=							
	14	=	=							
	15	=	=							
	16	=	=							
	17	=	=							
	18	=	=							
	19	=	=							
	20	=	=							

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/266,368	04/30/2014	Kevin J. Ma	P43758-US3

CONFIRMATION NO. 9269

27045
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

POA ACCEPTANCE LETTER

OC000000078098968

Date Mailed: 10/19/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/12/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/vnguyen/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/266,368	04/30/2014	2433	1600	P43758-US3	20	2

CONFIRMATION NO. 9269
REPLACEMENT FILING RECEIPT

27045
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

OC000000078099112

Date Mailed: 10/19/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Kevin J. Ma, Nashua, NH;
Robert Hickey, Bedford, MA;
Paul Tweedale, Andover, MA;

Applicant(s)

Ericsson AB, Stockholm, SWEDEN;

Power of Attorney: The patent practitioners associated with Customer Number 27045

Domestic Priority data as claimed by applicant

This application is a CON of 13/530,997 06/22/2012 PAT 8751807
which claims benefit of 61/500,316 06/23/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 05/15/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/266,368**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/AIA/122 (08-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Application

Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	14/266,368
Filing Date	April 30, 2014
First Named Inventor	Kevin J. Ma
Art Unit	2433
Examiner Name	Hoffman, Brandon S.
Attorney Docket Number	P43758-US3

Please change the Correspondence Address for the above-identified patent application to:

[x] The address associated with Customer Number: 27045

OR

[ ] Firm or Individual Name

Address

City	State	Zip

Country

Telephone	Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

[ ] Applicant

[x] Attorney or agent of record. Registration Number 64,170.

[ ] Registered practitioner named in the application transmittal papers who acts in a representative capacity under 37 CFR 1.34. See 37 CFR 1.33(a)(1). Registration Number _____.

Signature / Ronald S. Liu /

Typed or Printed Name Ronald S. Liu

Date October 12, 2015	Telephone 972-583-5812

NOTE: This form must be signed in accordnace with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications.
Submit multiple forms if more than one signature is required, see below*.

[ ] *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

POWER OF ATTORNEY AND AUTHORISATION

We, the undersigned Ericsson AB, having our registered offices at SE-164 80 Stockholm, Sweden, do hereby authorise **Roger Burleigh,** Ericsson Inc, to authorise individuals or companies to represent us before the Swedish Patent and Registration Office or any other national or regional or international patent office or patent registration authority (in its capacity as a National patent office and as a Receiving Office or International Searching Authority or International Preliminary Examining Authority under the Patent Cooperation Treaty) and the Swedish administrative court Patentbesvärsrätten and Regeringsrätten in any matter regarding patents or utility models.

Any authorisation relating to one specific invention, patent application, patent, utility model application or utility model only may be signed by Roger Burleigh only. However, any authorisation applicable to more than one specific invention, patent application, patent, utility model application or utility model
shall be signed jointly by Gabriele Mohsler, Ericsson GmbH.
shall not include the right to make sub-authorisations,
shall not exclude the possibility of corresponding authorisations for others,
shall be possible to revoke at any time, and
shall be valid for five years unless earlier revoked.

Roger Burleigh is further authorised to singly and independently represent us before the Swedish Patent Office (in its capacity as the Swedish patent office and as a Receiving Office or International Searching Authority or International Preliminary Examining Authority under the Patent Cooperation Treaty) and the Swedish administrative courts Patentbesvärsrätten and Regeringsrätten in any matter regarding patents or utility models.

The authorisations set out herein relating to Patentbesvärsrätten and Regeringsrätten shall be deemed as "Rättegångsfullmakt" in accordance with the Swedish procedural laws Rättegångsbalken, Förvaltningsprocesslagen and Lagen om Patentbesvärsrätten.

Roger Burleigh is further authorised to sign on behalf of us any certificates, declarations or statements needed by applicable law or Patent Office rules for the filing or prosecution of our patent applications at any Patent Office.

Roger Burleigh is further authorised to accept and sign assignments between Telefonaktiebolaget LM Ericsson, or any of its subsidiaries or employee of the Ericsson Group companies of all their rights to an invention, a patent application, a patent, a utility model application or a utility model.

Stockholm, February 5th, 2014

ERICSSON AB,

Nina Macpherson
Senior Vice President
and General Counsel

Christina Petersson
Vice President and
Head of IPR

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
AZUKI SYSTEMS, INC.	06/25/2014

RECEIVING PARTY DATA

Name:	ERICSSON AB
Street Address:	TORSHAMNSGATEN 23
City:	STOCKHOLM
State/Country:	SWEDEN
Postal Code:	SE-172 81

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	14266368

CORRESPONDENCE DATA

Fax Number: (972)583-6567
Phone: 9725836567
Email: kathryn.lopez@ericsson.com
Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.
Correspondent Name: RONALD S. LIU
Address Line 1: 6300 LEGACY DRIVE
Address Line 4: PLANO, TEXAS 75024

ATTORNEY DOCKET NUMBER:	P43758-US3
NAME OF SUBMITTER:	RONALD S. LIU
Signature:	/Ronald S. Liu/

Date:	10/12/2015

Total Attachments: 4
source=P43758_Formal Documents_2015-10-12_Recorded Assignment (US3)#page1.tif
source=P43758_Formal Documents_2015-10-12_Recorded Assignment (US3)#page2.tif
source=P43758_Formal Documents_2015-10-12_Recorded Assignment (US3)#page3.tif
source=P43758_Formal Documents_2015-10-12_Recorded Assignment (US3)#page4.tif

RECEIPT INFORMATION

EPAS ID:	PAT3565252
Receipt Date:	10/12/2015

Azuki Technology Transfer Agreement and Assignment

This Azuki Technology Transfer Agreement and Assignment is by and between Azuki Systems Inc., a corporation organized under the laws of Delaware (below referred to as "Azuki"), and Ericsson AB, a corporation organized under the laws of Sweden (below referred to as "EAB"), and is dated June 25, 2014.

RECITALS:

Azuki is the owner of certain rights, title and interest in technical intellectual property (below referred to as the "Azuki Intellectual Property") used in its business operations.

EAB desires to acquire all of Azuki's rights, title and interest in the Azuki Intellectual Property for use in its business operations.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. The Azuki Intellectual Property means the combination of any and all software, copyrights, processes, patents, trade secrets, know-how and other technical intellectual property rights used or of value in the current or future operation of Azuki's business operations.

2. Azuki hereby sells, assigns and transfers to EAB, its success and assigns, any and all right, title and interest in and to the Azuki Intellectual Property, and any and all causes of action for past, present, and future infringement of such rights.

3. This transfer is effective as of the date first written above.

4. The purchase price for the Azuki Intellectual Property is US$ [redacted] EAB shall pay the purchase price to Azuki through the normal Ericsson intercompany payment procedures, as promptly as is reasonably possible.

5. Azuki shall take such other actions as are requested by EAB to evidence the transactions described in this Agreement and Assignment. Azuki shall provide, at EAB's direction, such electronic or other files, data bases, code or other information in such form and at such times as EAB shall reasonably request,

6. EAB shall defend and indemnify Azuki in any claim, suite or proceeding brought against Azuki alleging that the use of the Azuki Intellectual Property infringes any intellectual property right of a third party. Azuki shall promptly notify EAB of any such claim, suit or proceeding, allow EAB to control the defense thereof, and cooperate with EAB in the defense of the claim, suit or proceeding.

IN WITNESS WHEREOF, the Parties hereto cause this Agreement and Assignment to be executed on or before the date first written above.

AZUKI SYSTEMS, INC.	ERICSSON AB
By:_____	By:_____
Name:_____	Name: Roland Hagman
By:_____	By:_____
Name:_____	Name: Lars Molander

Azuki Technology Transfer Agreement and Assignment

This Azuki Technology Transfer Agreement and Assignment is by and between Azuki Systems Inc., a corporation organized under the laws of Delaware (below referred to as "Azuki"), and Ericsson AB, a corporation organized under the laws of Sweden (below referred to as "EAB"), and is dated June 25, 2014.

RECITALS:

Azuki is the owner of certain rights, title and interest in technical intellectual property (below referred to as the "Azuki Intellectual Property") used in its business operations.

EAB desires to acquire all of Azuki's rights, title and interest in the Azuki Intellectual Property for use in its business operations.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. The Azuki Intellectual Property means the combination of any and all software, copyrights, processes, patents, trade secrets, know-how and other technical intellectual property rights used or of value in the current or future operation of Azuki's business operations.

2. Azuki hereby sells, assigns and transfers to EAB, its success and assigns, any and all right, title and interest in and to the Azuki Intellectual Property, and any and all causes of action for past, present, and future infringement of such rights.

3. This transfer is effective as of the date first written above.

4. The purchase price for the Azuki Intellectual Property is US$[redacted]. EAB shall pay the purchase price to Azuki through the normal Ericsson intercompany payment procedures, as promptly as is reasonably possible.

5. Azuki shall take such other actions as are requested by EAB to evidence the transactions described in this Agreement and Assignment. Azuki shall provide, at EAB's direction, such electronic or other files, data bases, code or other information in such form and at such times as EAB shall reasonably request,

6. EAB shall defend and indemnify Azuki in any claim, suite or proceeding brought against Azuki alleging that the use of the Azuki Intellectual Property infringes any intellectual property right of a third party. Azuki shall promptly notify EAB of any such claim, suit or proceeding, allow EAB to control the defense thereof, and cooperate with EAB in the defense of the claim, suit or proceeding.

IN WITNESS WHEREOF, the Parties hereto cause this Agreement and Assignment to be executed on or before the date first written above.

AZUKI SYSTEMS, INC.

By: _____

Name: KEVIN DURKIN

By: _____

Name: _____

ERICSSON AB

By: _____

Name: _____

By: _____

Name: _____

Electronic Acknowledgement Receipt

EFS ID:	23754050
Application Number:	14266368
International Application Number:	
Confirmation Number:	9269
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Customer Number:	47654
Filer:	Steven Ware Smith/Kathryn Lopez
Filer Authorized By:	Steven Ware Smith
Attorney Docket Number:	1082-018.002
Receipt Date:	12-OCT-2015
Filing Date:	30-APR-2014
Time Stamp:	13:52:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	P43758-US3_2015-10-12_15-9598_Supplemental_ADS.pdf	1449734 71051646bcce4a4bc76ecce849e34cdd9fce381e	no	6

Warnings:

Information:

This is not an USPTO supplied ADS fillable form					
2		P43758-US3_2015-10-12_15-9598_PoA_and_CoA.pdf	1216832 2c78d2c951130a7dd8e3722eebe50f2fae26cf67	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Change of Address	1	1
	Power of Attorney	2	2
	Assignee showing of ownership per 37 CFR 3.73	3	4
	Power of Attorney	5	5
	Assignee showing of ownership per 37 CFR 3.73	6	11

Warnings:

Information:

Total Files Size (in bytes):	2666566

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	[redacted] P43758-US3
	Application Number	14/266,368
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Kevin	J.	Ma	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Nashua	State/Province	NH	Country of Residence	US

Mailing Address of Inventor:

Address 1	16 Bicentennial Drive		
Address 2			
City	Nashua	State/Province	NH
Postal Code	03062	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Robert		Hickey	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Bedford	State/Province	MA	Country of Residence	US

Mailing Address of Inventor:

Address 1	2 Fawn Circle		
Address 2			
City	Bedford	State/Province	MA
Postal Code	01730	Country i	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Paul		Tweedale	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	[redacted] P43758-US3
	Application Number	14/268,368
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

City	Andover	State/Province	MA	Country of Residence	US

Mailing Address of Inventor:

Address 1	150 Shawsheen Road		
Address 2			
City	Andover	State/Province	MA
Postal Code	01810	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence information of this application.**

Customer Number	[redacted] 27045		
Email Address	[redacted]	Add Email	Remove Email

patent.development@ericsson.com

Application Information:

Title of the Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY		
Attorney Docket Number	[redacted] P43758-US3	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	3	Suggested Figure for Publication (if any)	3

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	[redacted]02 P43758-US3
	Application Number	14/266,368
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	[redacted]54 27045		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13530997	2012-06-22
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13530997	Claims benefit of provisional	61500316	2011-06-23

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[1] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[1]	Filing Date (YYYY-MM-DD)	Access Code[1] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	[redacted] P43758-US3
	Application Number	14/266,368
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	[redacted]2 P43758-US3
	Application Number	14/266,368
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(●) Assignee ( ) Legal Representative under 35 U.S.C. 117 ( ) Joint Inventor

( ) Person to whom the inventor is obligated to assign. ( ) Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	[redacted] Ericsson AB		
Mailing Address Information For Applicant:			
Address 1	[redacted] Torshamnsgaten 23		
Address 2	[redacted]		
City	[redacted] Stockholm	State/Province	[redacted]
Country	[redacted] SE	Postal Code	[redacted] SE-172 81
Phone Number		Fax Number	
Email Address	patent.development@ericsson.com		

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	[redacted] P43758-US3
	Application Number	14/266,368
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Signature	/ Ronald S. Liu, Reg. No. 64170 /			Date (YYYY-MM-DD)	2015-10-12
First Name	Ronald	Last Name	Liu	Registration Number	64170

Additional Signature may be generated within this form by selecting the Add button.

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

[■] Practitioners associated with Customer Number: 27045

OR

[ ] Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

[■] The address associated with Customer Number: 27045

OR

Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address: Ericsson AB
Torshamnsgaten 23
Stockholm, Sweden SE-172 81

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	/Roger S. Burleigh/	Date	October 12, 2015
Name	Roger S. Burleigh	Telephone	972-583-5799
Title	Secretary, Ericsson AB		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Ericsson AB

Application No./Patent No.: 14/266,368 Filed/Issue Date: April 30, 2014

Titled: METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

Ericsson AB, a Swedish Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Roger S. Burleigh/	October 12, 2015
Signature	Date
Roger S. Burleigh	Secretary, Ericsson AB
Printed or Typed Name	Title or Registration Number

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kevin J. Ma, et al.	§	Group Art Unit:	2433
		§		
Application No:	14/266,368	§	Examiner:	Hoffman, Brandon S.
		§		
Filed:	April 30, 2014	§	Confirmation No:	9269
		§		

Attorney Docket No: P43758-US3
Customer No.: 27045

For: **METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY**

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for First class or Express mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or being facsimile transmitted to the USPTO at (571) 273-8300 or being transmitted via EFS-Web on the date indicated below.

Date: **August 26, 2015**

Name: **Kathryn Lopez**

Signature: /Kathryn Lopez/

Dear Examiner:

Response to Non-Final Office Action

REPLY UNDER 37 CFR § 1.111

In response to the Non-Final Office Action dated May 26, 2015, Applicant submits the following remarks and/or amendments on or before the expiration of the three-month shortened statutory period for reply (August 26, 2015). If any extension of time for this Response is required, Applicant requests that this be considered a petition therefor. The Commissioner is hereby authorized to charge any additional fee to Deposit Account No. 50-1379.

1.) The Specification has been amended and begins on page 2 of this paper.

2.) Remarks/Arguments begin on page 3 of this paper.

Amendments to the Specification:

Please add the following new paragraph after the title of the application ending on line 2 of page 1:

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Application No. 61/500,316, filed June 23, 2011, and U.S. Patent Application No.: 13/530,997, filed on June 22, 2012 now U.S. Patent No. 8,751,807. The content of the above applications are incorporated by reference in their entirety.

REMARKS/ARGUMENTS

1.) Status of the Claims

Claims 1-20 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the following remarks.

2.) Examiner Objections – Specification

Applicant has amended the Specification to address Examiner's objection.

3.) Allowable Subject Matter

The Applicant gratefully acknowledges the allowance of claims 1-20.

CONCLUSION

In view of the foregoing remarks, Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. Applicant, therefore, respectfully requests that Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

Applicant requests a telephonic interview if Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

/ Ronald S. Liu, Reg. No. 64,170 /

Ronald S. Liu
Registration No. 64,170

Date: August 26, 2015

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8512
ronald.liu @ericsson.com

Electronic Acknowledgement Receipt

EFS ID:	23313756
Application Number:	14266368
International Application Number:	
Confirmation Number:	9269
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	Kevin J. Ma
Customer Number:	47654
Filer:	Steven Ware Smith/Kathryn Lopez
Filer Authorized By:	Steven Ware Smith
Attorney Docket Number:	1082-018.002
Receipt Date:	26-AUG-2015
Filing Date:	30-APR-2014
Time Stamp:	11:36:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P43758-US3_2015-08-26_15-3652_Response_to_NFOA_dated_05-26-2015.pdf	77607 703edf32949ecad0c778287be9614cd382290670	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	77607	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/266,368	04/30/2014	Kevin J. Ma	1082-018.002	9269

47654 7590 05/26/2015
BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
05/26/2015	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No. 14/266,368	Applicant(s) MA ET AL.	
	Examiner BRANDON HOFFMAN	Art Unit 2433	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *April 30, 2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *1-20* is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☒ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *April 30, 2014* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *4-30-14*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

1. Claims 1-20 are pending in this office action.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on April 30, 2014, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

3. The disclosure is objected to because of the following informalities: the CROSS-REFERENCE TO RELATED APPLICATIONS section is missing. Appropriate correction is required.

Allowable Subject Matter

1. Claims 1-20 are allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRANDON HOFFMAN/
Primary Examiner, Art Unit 2433

Notice of References Cited	Application/Control No. 14/266,368	Applicant(s)/Patent Under Reexamination MA ET AL.	
	Examiner BRANDON HOFFMAN	Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0060316	03-2005	Kamath et al.	707/009
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9269

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/266,368	04/30/2014 **RULE**	713	2433	1082-018.002

APPLICANTS
Azuki Systems, Inc., Acton, MA;

INVENTORS
Kevin J. Ma, Nashua, NH;
Robert Hickey, Bedford, MA;
Paul Tweedale, Andover, MA;

**** CONTINUING DATA ***************************
This application is a CON of 13/530,997 06/22/2012 PAT 8751807
which claims benefit of 61/500,316 06/23/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
05/15/2014

			STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /BRANDON S HOFFMAN/ Examiner's Signature	☐ Met after Allowance Initials		NH	3	20	2

ADDRESS

BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581
UNITED STATES

TITLE

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

FILING FEE RECEIVED 1600	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

14266368 - GAU: 2433
PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	2014-04-30
	First Named Inventor	Kevin J. Ma
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1082-018.002

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070038857	A1	2007-02-15	Gosnell	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2010108053	WO	A1	2010-09-23	Azuki Systems, Inc.		☐
	2	2011020088	WO	A1	2011-02-17	Azuki Systems, Inc.		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS	Remove

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.H./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14266368 - GAU: 2433
	Filing Date	2014-04-30
	First Named Inventor	Kevin J. Ma
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1082-018.002

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	PANTOS ET AL., HTTP Live Streaming, downloaded from http://tools.ietf.org/html/draft-pantos-http-live-streaming-06, published March 31, 2011.	☐
	2	MICROSOFT CORPORATION, Using Silverlight DRM, Powered by PlayReady, with Windows Media DRM Content, downloaded from http://download.microsoft.com/download/7/6/D/76D540F7-A008-427C-8AFC-BE9E0C0D8435/ Using_Silverlight_with_Windows_Media_DRM-Whitepaper_FINAL.doc, published November 2008.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Brandon Hoffman/	Date Considered	05/12/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.H./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14266368 - GAU: 2433
	Filing Date	2014-04-30
	First Named Inventor	Kevin J. Ma
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1082-018.002

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James F. Thompson/	Date (YYYY-MM-DD)	2014-04-30
Name/Print	James F. Thompson, Esq.	Registration Number	36,699

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.H./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.H./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L17	18174	key near rotat$4	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:16
L18	153543	streaming	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:16
L19	4780	encrypt$3 with expir$5	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:16
L20	30	L17 and L18 and L19	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:16
L21	162721	playback	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:26
L22	74552	encryption near key	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:26
L23	10911	key near identifier	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:27
L24	153106	expiration	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:27
L25	189406	manifest	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:27
L26	3499	license near server	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:27
L27	8827	key near rotation	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:27
L28	3	21 and 22 and 23 and 24 and 25 and 26 and 27	US-PGPUB; USPAT; USOCR	OR	ON	2015/05/18 15:27

EAST Search History (Interference)

<This search history is empty>

5/18/2015 3:28:22 PM
C:\Users\bhoffman\Documents\EAST\Workspaces\14266368.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/12/2015								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	=								
	11	=								
	12	=								
	13	=								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	=								
	20	=								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14266368	MA ET AL.
	Examiner	**Art Unit**
	BRANDON HOFFMAN	2433

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
713	168 - with keyword limiters	5-12-15	BH

SEARCH NOTES

Search Notes	Date	Examiner
inventor name search	5-12-15	BH
see attached EAST search notes	5-12-15	BH

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/BRANDON HOFFMAN/ Primary Examiner.Art Unit 2433

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/266,368	04/30/2014	Kevin J. Ma	1082-018.002

CONFIRMATION NO. 9269

PUBLICATION NOTICE

47654
BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

OC000000070322349

Title:METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

Publication No.US-2014-0237243-A1
Publication Date:08/21/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/266,368	04/30/2014	2431	1600	1082-018.002	20	2

CONFIRMATION NO. 9269

FILING RECEIPT

47654
BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
WESTBOROUGH, MA 01581

OC000000068467001

Date Mailed: 05/15/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Kevin J. Ma, Nashua, NH;
Robert Hickey, Bedford, MA;
Paul Tweedale, Andover, MA;

Applicant(s)

Azuki Systems, Inc., Acton, MA

Assignment For Published Patent Application

Azuki Systems, Inc., Acton, MA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/530,997 06/22/2012
which claims benefit of 61/500,316 06/23/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 05/15/2014
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/266,368**
Projected Publication Date: 08/21/2014
Non-Publication Request: No
Early Publication Request: No

Title

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

Preliminary Class

380

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/266,368

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1600

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	2014-04-30
	First Named Inventor	Kevin J. Ma
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1082-018.002

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070038857	A1	2007-02-15	Gosnell	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2010108053	WO	A1	2010-09-23	Azuki Systems, Inc.		☐
	2	2011020088	WO	A1	2011-02-17	Azuki Systems, Inc.		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS	Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2014-04-30
	First Named Inventor	Kevin J. Ma
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1082-018.002

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	PANTOS ET AL., HTTP Live Streaming, downloaded from http://tools.ietf.org/html/draft-pantos-http-live-streaming-06, published March 31, 2011.	☐
	2	MICROSOFT CORPORATION, Using Silverlight DRM, Powered by PlayReady, with Windows Media DRM Content, downloaded from http://download.microsoft.com/download/7/6/D/76D540F7-A008-427C-8AFC-BE9E0C0D8435/ Using_Silverlight_with_Windows_Media_DRM-Whitepaper_FINAL.doc, published November 2008.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2014-04-30
	First Named Inventor	Kevin J. Ma
	Art Unit	
	Examiner Name	
	Attorney Docket Number	1082-018.002

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James F. Thompson/	Date (YYYY-MM-DD)	2014-04-30
Name/Print	James F. Thompson, Esq.	Registration Number	36,699

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2010 (23.09.2010)

PCT

(10) International Publication Number
WO 2010/108053 A1

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2010/027893

(22) International Filing Date:
19 March 2010 (19.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/161,641 19 March 2009 (19.03.2009) US
61/265,391 1 December 2009 (01.12.2009) US

(71) Applicant *(for all designated States except US)*: **AZUKI SYSTEMS, INC.** [US/US]; 43 Nagog Park, Suite 105, Acton, MA 01720 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MA, Kevin, J.** [US/US]; 16 Bicentennial Drive, Nashua, NH 03062 (US). **XU, Jianguo** [CN/US]; 30 Grant Street, Newton, MA 02465 (US). **NG, Tung** [US/US]; 50 Willow Ridge Road, North Andover, MA 01845 (US). **NAIR, Raj** [US/US]; 6 Burroughs Road, Lexington, MA 02420 (US). **LIN, Ichang** [US/US]; 24 Walker Street, Westborough, MA 01581 (US). **LI, Man** [CA/US]; 3 Overlook Drive, Bedford, MA 01730 (US).

(74) Agent: **THOMPSON, James, F.**; Bainwood Huang & Associates LLC, Highpoint Center, 2 Connector Road, Westborough, MA 01581 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: METHOD FOR SCALABLE LIVE STREAMING DELIVERY FOR MOBILE AUDIENCES

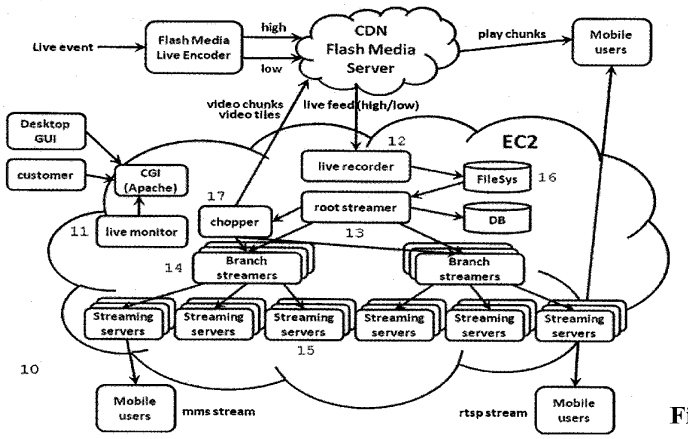


Fig. 2

(57) Abstract: A live streaming system/method provides cross platform live streaming capabilities to mobile devices. A file format compatible with legacy HTTP infrastructure is used to deliver media over a persistent connection. Legacy client media players can dynamically change the encoded rate of the media delivered over a persistent connection. Standard HTTP servers may be used without modification, leveraging standard media players embedded in mobile devices for seamless media delivery over wireless networks with high bandwidth fluctuations.

WO 2010/108053 A1

METHOD FOR SCALABLE LIVE STREAMING DELIVERY FOR MOBILE AUDIENCES

BACKGROUND

The invention relates generally to the field of streaming media, and more particularly to the streaming of live media in a scalable and flexible manner.

Available bandwidth in the internet can vary widely. For mobile networks, the limited bandwidth and limited coverage, as well as wireless interference can cause large fluctuations in available bandwidth which exacerbate the naturally bursty nature of the internet. When congestion occurs, bandwidth can degrade quickly. For streaming media, which require long lived connections, being able to adapt to the changing bandwidth can be advantageous. This is especially so for streaming which requires large amounts of consistent bandwidth.

In general, interruptions in network availability where the usable bandwidth falls below a certain level for any extended period of time can result in very noticeable display artifacts or playback stoppages. Adapting to network conditions is especially important in these cases. The issue with video is that video is typically compressed using predictive differential encoding, where interdependencies between frames complicate bit rate changes. Video file formats also typically contain header information which describe frame encodings and indices; dynamically changing bit rates may cause conflicts with the existing header information. This is further complicated in live streams where the complete video is not available to generate headers from.

Frame-based solutions like RTSP/RTP solve the header problem by only sending one frame at a time. In this case, there is no need for header information to describe the surrounding frames. However RTSP/RTP solutions can result in poorer quality due to UDP frame loss and require network support for UDP firewall fixups, which may be viewed as network security risks. More recently segment-based solutions like HTTP Live Streaming allow for the use of the ubiquitous HTTP protocol which does not have the frame loss or firewall issues of RTSP/RTP, but does require that the client media player support the specified m3u8 playlist polling. For many legacy mobile devices that support RTSP, and not m3u8 playlists, a different solution is required.

SUMMARY

A method and apparatus are disclosed for delivering live content (live video and/or audio) as streaming media over the Internet to mobile devices in a device- and operator-agnostic manner. Currently, mobile video broadcasting either uses a built-in capability which is specific to a particular cell network operator or requires a device-specific application download. The disclosed technique may be used with a standard web-browser and delivered via the Internet to any mobile device in a manner that is independent of any particular cell network operator. The technique can efficiently scale horizontally to a large number of endpoints (mobile devices). In addition, a capability for automatically saving and viewing earlier segments of the stream is also provided. Overall, the disclosed method and apparatus provide the ability to deliver, in a scalable and cost-effective manner, live and time-shifted streaming of content over the Internet to mobile endpoints.

In one general respect, a disclosed system includes functions of recording, transcoding, and distributing live content or media. A recording system captures the live stream and transcodes it to various mobile device formats such as 3gpp, WMV, MOV, etc. and may dynamically segment a copy of the live stream into "chapters" for time-shifted viewing. Segments may also be used to support downloading at selectable data rates. The transcoded data is stored in a file system. A distribution subsystem provides distribution to a large number of endpoints in a highly scalable manner. In particular, a distribution tree may be employed for which the number N of endpoints is less than or equal to F^h, where F is the "fanout" or number of branches exiting each node and h is the height (number of levels) of the tree. Note that h grows only logarithmically in relation to N.

In another respect, the disclosed system records data into segments, in a plurality of encodings in a plurality of formats, to support a plurality of heterogeneous client devices. In one embodiment, the source video is transcoded into a plurality of different bit rate encodings, which are written into separate files in segments. In one embodiment, each bit rate encoding may be stored in a plurality of file formats. Each format is written to a separate segment file. The different bit rates may be used to support heterogeneous client devices generally, as well as provide the ability for adaptive adjustment of the bandwidth required for downloading to tailor operation to changing network conditions, improving overall system performance.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages will be apparent from the following description of particular embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of various embodiments of the invention.

Figure 1 is a high-level block diagram of a system for delivery of live content streams to a number of mobile devices;

Figure 2 is a block diagram of the system of Figure 1 showing detail of a live streaming system component;

Figure 3 is a block diagram of a system which is capable of conducting procedures, in accordance with various embodiments of the invention;

Figure 4 is a diagram of a live stream recording and segmentation server, in accordance with various embodiments of the present invention;

Figure 5 is a diagram of a segment file format, in accordance with an embodiment of the present invention;

Figure 6 is a diagram of a native RTSP live streaming client capable of viewing live segments, in accordance with an embodiment of the present invention;

Figure 7 is a diagram of a native HTTP live streaming client capable of viewing live segments, in accordance with an embodiment of the present invention;

Figure 8 is a flow chart showing a method for performing live stream segmentation, in accordance with various embodiments of the invention;

Figure 9 is a flow chart showing a method for performing live stream segment retrieval and decoding, in accordance with an embodiment of the present invention; and

Figure 10 is a flow chart showing a method for performing live stream segment retrieval and decoding, in accordance with another embodiment of the present invention.

DETAILED DESCRIPTION

Overview

A scalable live streaming system is used to deliver live event to large mobile audiences. The system generally provides mobile users with interactive and "snackable" access to the content, i.e., the ability to view selected portions of the content, along with

metadata associated within a live event. The system supports the following major live streaming features:

- Live Streaming

Live streaming provides real time live streaming functionality. In one embodiment, the system receives the live feed as a live stream from a content delivery network (CDN). In another embodiment, the system receives the live feed as a direct stream from an attached recording device (e.g. a web-cam). The stream is recorded into a media file and re-streamed out with different encoding formats to support different mobile audiences.

- Interactive Near-Live Streaming

In one embodiment, the system provides near-live interactive streaming functionality for a live feed. A mobile user can navigate the live event and play interesting video chunks in near real time while the live event is ongoing. In one embodiment, the system supports redirecting from a near live chunk to the live streaming to allow a mobile user to “tune” in the live event directly.

- Server-side Simulated Broadcast Live Streaming

This feature allows an end-user to tune in the live streaming event anywhere from the beginning of live event to near the present time.

- Video on Demand

In one embodiment, the live event is recorded by the system. The recorded file can be further transcoded into multiple media formats to provide Video on Demand (VoD) replay functionality after the live event is over.

As used herein, "near-live" refers to the presence of certain latencies in the system, such as recording the live stream(s), transcoding the live media, relaying an intermediate stream, chopping into video chunks, extracting image "tiles", and transferring the video chunks to a content delivery network. The particular constituents and amounts of these delays will necessarily vary among different embodiments.

The system may also provide a desktop graphical user interface (GUI) to control operation such as starting and stopping a stream.

In another aspect, the disclosed system records data into segments, in a plurality of encodings in a plurality of formats, to support a plurality of heterogeneous client devices. In

one embodiment, the source video is transcoded into a plurality of different bit rate encodings. The plurality of encodings are written into separate files, in segments. In one embodiment, each bit rate encoding may be stored in a plurality of file formats. Each format is written to a separate segment file. In one embodiment, the segment files adhere to a file naming convention which specifies the bit rate and format in the name, to simplify segment retrieval. The segment-based technique may be one general method by which the live stream is downloaded to the mobile endpoint devices (which are also referred to as "clients" herein).

In one embodiment, the segments contain recorded and transcoded video data. In another embodiment, the segments may contain non-video data which has been compressed and encrypted using different encoding methods to produce a plurality of encodings. The different compression and encryption methods may require different levels of complexity and different amounts of client resources to reconstruct. Different compression and encryption schemes provide different levels of quality (i.e. higher or lower compression and higher or lower security); they also have different types of framing and format organization, the details of which should be known to those skilled in the art.

In one embodiment, the segments are all of a fixed duration. In another embodiment, the segments may all be of a fixed size. In one embodiment, video segments are packed to integer time boundaries. In another embodiment compressed and/or encrypted segments are padded out to round numbered byte boundaries. This can help simplify byte-based offset calculations. It also can provide a level of size obfuscation, for security purposes. In another embodiment the segments may be of variable duration or size. In one embodiment, video segments are packed based on key frame or group of frame counts.
In one embodiment, the segments are served from standard HTTP servers. In another embodiment, the segments may be served from an optimized caching infrastructure. The segments are designed to be usable with existing infrastructure. They do not require special servers for delivery and they do not require decoding for delivery. They also do not require custom rendering engines for displaying the content.

In one embodiment, a native client media player may be used as the rendering engine. In another embodiment, a custom rendering engine may be used.

In one embodiment, a progressive downloader can be employed to manage a data buffer. A network proxy feeds the buffered data to the rendering engine. In one

embodiment, the downloader uses simple HTTP requests to retrieve complete segments as pre-segmented data files. In another embodiment, the downloader uses HTTP range GETs to retrieve segments of data from a larger file. The segments are retrieved as they become available from the live media source. In another embodiment, other legacy data retrieval methods are used, e.g. FTP. In one embodiment the downloader starts with the newest segment to provide as near to live viewing as possible. In another embodiment the downloader may start with older segments to support seeking, increase protection against network interruption or to start from a fixed point.

In one embodiment, the downloader measures network bandwidth based on the round trip download time for each segment as (S / T), where S is the size of the segment and T is the time elapsed in retrieving the segment. This includes the latency associated with each request. For video media using fixed duration segments, as available bandwidth decreases and rate adaptation is employed, the total bytes per segment will decrease. As this congestion occurs, request latency overhead increases, which helps to predict rapid downward changes in bandwidth.

In one embodiment, the downloader keeps a trailing history of B bandwidth estimates, calculating the average over the last B samples. When a new sample is taken, the Bth oldest sample is dropped and the new sample is included in the average. The following pseudocode provides an illustration:

```
integer B_index    // tail position in the circular history buffer
integer B_total    // sum of all the entries in the history buffer
integer B_count    // total number of entries in the history buffer
integer B_new      // newly sampled bandwidth measurement
integer B_old      // oldest bandwidth sample to be replaced
integer B_average  // current average bandwidth
array B_history    // circular history buffer

B_old = B_history[B_index]         // find the sample to be replaced
B_history[B_index] = B_new         // replace the sample with the new sample
B_total = B_total - B_old          // remove the old sample from the sum
B_total = B_total + B_new          // add the new sample into the sum
B_average = B_total / B_count      // update the average
B_index = (B_index + 1) % B_count  // update the buffer index
```

The history size may be selected so as not to tax the client device. A longer history will be less sensitive to transient fluctuations, but will be less able to predict rapid decreases in bandwidth. In another embodiment the downloader keeps only a single sample and uses a dampening filter for statistical correlation. The following provides illustrative pseudocode:

```
integer B_new      // newly sampled bandwidth measurement
integer B_average  // current average bandwidth
```

```
float B_weight     // weight of new samples, between 0 and 1

B_average = (B_average * (1 - B_weight)) + (B_average * B_weight) // update the
average
```

This method may require less memory and fewer calculations. It can also allow for exponential drop off in historical weighting.

In one embodiment, download progress for a given segment is monitored periodically so that the segment size S of the retrieved data does not impact the rate at which bandwidth measurements are taken. There are numerous methods for estimating bandwidth, as should be known to those skilled in the art; the above are representative of the types of schemes possible but do not encompass an exhaustive list of schemes. Other bandwidth measurement techniques as applicable to the observed traffic patterns are acceptable within the context of the present invention.

In one embodiment, bandwidth measurements are used to determine when a change in bit rate is required. If the estimated bandwidth falls below a given threshold for the current encoding, for a specified amount of time, then a lower bit rate encoding should be selected. Likewise if the estimated bandwidth rises above a different threshold for the current encoding, for a different specified amount of time, then a higher bit rate encoding may be selected. The rate change takes place at the download of the next segment.

Description of Illustrative Embodiments

Figure 1 shows a block diagram of a live media streaming environment which includes mobile users and a "mash media platform" residing in an elastic compute cloud (EC2). A live media stream (e.g., of a live event) is generated by a live media source. A live streaming system 10 receives the live event media stream from a content delivery network (CDN) and delivers corresponding live media streams and interactive "near-live" streams to mobile audiences. Various formats of incoming live streams can be supported, including Flash format.

The live streaming system provides the following functionality:

- Control live streaming system starting and stopping.
- Interface with external live feed.
- Record the live stream(s) into local media file(s).
- Transcode recorded file into different encoding formats supported by the system.

- Chop recorded media file into video chunks with predefined chunk duration.
- Extract image tiles from the recorded media file with predefined tile interval.
- Upload the video chunks to CDN in real time.
- Support existing user interaction functionality for the live event.
- Support RTSP and MMS streaming for mobile devices.
- Create metadata associated with the live event.
- Create server-side playlist and SDP files for simulated server side live broadcasting.

The live streaming system is designed to be flexible and easily expandable to support large mobile audiences.

Figure 2 shows the overview of the live streaming system 10. The system includes a Live Streaming Monitor 11 (shown as "live monitor"), a Live Streaming Recorder 12 ("live recorder"), Root Streamer 13, Branch Streamers 14, and Streaming Servers 15. These are now described in turn. It will be appreciated that these components may correspond to software being executed by one or a collection of computerized devices, as that term is more fully defined below.

Live Streaming Monitor and Control

The live streaming monitor 11 consists of scripts running in the background to monitor incoming stream properties, the status of an RTMP connection, and the status of the Root Streamer 13 and Branch Streamers 14. Additionally, a Web-based interface is provided in the system to be used by a customer to send stream properties before the live event starts or end of the live event. In one embodiment, the Web-based interface is implemented as a CGI script. In another embodiment, the Web-based interface is implemented as a RESTful Web Service. A desktop GUI may be provided to control the live streaming server by calling the Web-based interface. An example CGI interface may be the following:

http://<hostname>/cgi-bin/ags.cgi?event=<name>&id=<event id>&status=<on|off>

where a customer provides the following parameters:

- event: stream name
- id: event ID

- status: event status (ON or OFF)

These scripts control the whole live streaming system to start, stop, and terminate automatically based on stream properties and network connection status. A system administrator can also control the system through GUI.

Live Streaming Recorder

In one embodiment, the Live Stream Recorder 12 is used to capture a live stream via the RTMP protocol and save the stream into a local file. In another embodiment, the Live Stream Recorder 12 is used to capture a live stream via the MMS protocol and save the stream to a local file. In another embodiment, the Live Stream Recorder 12 is used to capture a live stream via the RTP protocol and save the stream to a local file. The local file can be one of a number of valid container formats (e.g. FLV, MP4, 3GP, MOV, WMV, etc.) which should be known to those skilled in the art. The local file is then transcoded and streamed out through the Streaming Tree (described below). The Live Stream Recorder 12 is also responsible for notifying the Live Stream Monitor of streaming protocol specific events which affect the state of the stream (e.g. stream start, stream stop, and stream errors).

Video on Demand

The live event is recorded by the Live Streaming Recorder 12 into a recorded media file. This media file can be further transcoded into multiple transcoded media files in different formats. These transcoded media files can be used by the system to provide Video on Demand (VoD) functionality after the live event is over.

Live Event Metadata and Database (shown as "DB" in Figure 2)

While a live event is ongoing, multiple metadata associated with the live event are created and stored in the central database 16. These metadata can be used to describe the properties of each specific live event. By using these metadata entries in the database, each live event is searchable.

Streaming Tree

A Streaming Tree contains at least one Root Streamer 13 and multiple Streaming Servers 15. One or more intermediate Branch Streamers 14 are generally also employed, although for sufficiently small audiences it may be possible for the Root Streamer 13 to provide its streams directly to Streaming Servers15. Each Streaming Tree is used to deliver one live event. The Branch Streamers 14 and Streaming Server 15 receive streams from their parents and replicate the stream to multiple children. Within one Streaming Tree, more Branch Streamers 14 and Streaming Servers 15 can be added into the Streaming Tree to accommodate the mobile audience scale. A Streaming Tree is one specific type of stream distribution subsystem. For VoD or chunk content, the Streaming Tree may function more as a hierarchical caching infrastructure with push-based distribution of live recorded files. In one embodiment, Streaming Tree distribution is performed by unicast connections between parents and children. In another embodiment, Streaming Tree distribution is performed via IP multicast.

Multiple Live Events

The system can be easily expanded to support concurrent live events. The system can be configured to have multiple Streaming Trees each delivering a different live event. Multiple Streaming Trees may also be used to provide different encodings of a single live event. For VoD or chunk content, a single distribution tree may be used to support multiple encoding or live events.

Encoding Parameters Configuration

When a live event is starting, a set of encoding parameters, such as, video format, video bit rate, audio format, audio bit rate, frame rate, etc., can be configured to deliver specific streams to mobile audiences based on targeted mobile phones and wireless network bandwidth. These encoding parameters have been configured to support various mobile phones and wireless carrier networks.

Load Balancing

The system can provide load balancing functionality to deliver the live stream to mobile users. The plurality of Streaming Servers 15 may be distributed across multiple data

centers, in which case DNS load balancing may be used to map the closest data center. Within a single data center, the plurality of Streaming Servers 15 may also be load balanced by a server load balancer to distribute load.

Live Streaming Navigation

The system may enable a user to watch a live event in two different ways. One is to watch the real time live event in the normal linear fashion (beginning to end). Another way is to allow the user to navigate into the live event to find interesting points and watch "snackable" portions or clips. These snackable clips are produced by the Live Streaming Chopper (see below) dynamically while the live event is ongoing.

Root Streamer

The Root Streamer 13 is the streaming source of the live streaming system. It transcodes the recorded l file and streams out multiple streams to either the intermediate Branch Streamers 14 or the Streaming Servers 15 directly. In one embodiment, the Root Streamer 13 uses RTP streams to distribute live content. The Root Streamer 13 also streams the live content to the chopper 17. The Root Streamer 13 also sets the event metadata to database so that the GUI can display the event status to mobile audiences.

There may be multiple Root Streamers 13 in the system in case of supporting multiple live streaming channels or multiple live stream encodings for one customer or many customers. By supporting multiple Root Streamers 13 and intermediate Branch Streamers 14, the system can support multiple customers and expand to support large audiences.

Branch Streamer

The Branch Streamer 14 is the intermediate streamer in the system. It takes the incoming RTP stream and relays the stream to a next level of the Branch Streamers 14 or to the Streaming Servers 15. The Branch Streamers 14 are used to expand the system to support large mobile audiences.

Streaming Server

The Streaming Servers 15 are the front end of the live streaming system to deliver the stream(s) to mobile audiences. They receive the streams from the Root Streamer 13 or Branch Streamers 14 and relay the streams to mobile audiences to watch the live event. The system may support a variety of streaming protocols, including but not limited to HTTP Live Streaming, RTSP and MMS. The number of Streaming Servers 15 used will generally depend on how many concurrent clients are supported by the live streaming system. Additional Streaming Servers 15 may also be used to provide physical distribution over a wider geographical area. Increasing distribution allows for lower latency when streaming to mobile clients in a specific region. The streams delivered to the client devices by the Streaming Servers are referred to as "distributed streams".

Live Streaming Chopper

The Live Streaming Chopper 17 is used for the interactive Near-Live Streaming. It receives the stream from Root Streamer 13, transcodes and saves the stream to many N-minute video chunks, chops the N-minute video chunks into smaller video chunks based on a default definition file and extracts image tiles. In one embodiment, the Chopper 17 uploads chunks and tiles to a CDN for distribution to clients. In another embodiment, the Chopper 17 uses the Streaming Tree as a distribution path for video chunks. In one embodiment the chunks are distributed using reliable multicast to the Branch Streamers (or proxy caches in this case) 14, through to the Streaming Servers 15.. In one embodiment, the user can play the snackable chunks through an interactive GUI such as described in PCT patent application PCT/US09/32565 entitled "Media Navigation System", published August 6, 2009 as WO/2009/097492. In another embodiment, the user can play the chunks using an HTTP Live Streaming compatible media player. In another embodiment, the user can play the chunks using a method in accordance with various provisions of this invention.

Figure 3 is a block diagram 100 for one embodiment of the present invention. It shows the client device 108 and live stream recording and segmentation (R/S) server 102 (which is referred to as "Live Stream Recorder" above). The R/S server 102 and client 108 are both typically computerized devices which include one or more processors, memory, storage (e.g., magnetic or flash memory storage), and input/output circuitry all coupled

together by one or more data buses, along with program instructions which are executed by the processor out of the memory to perform certain functions which are described herein. Part or all of the functions may be depicted by corresponding blocks in the drawings, and these should be understood to cover a computerized device programmed to perform the identified function.

The client 108 connects to a standard HTTP server 106 to retrieve segments. The segments are stored on a storage device 104. The storage may be local or remote and may use any of a number of storage technologies, as should be known to those skilled in the art. The segments are generated by the R/S server 102. The R/S server 102 is responsible for recording the live stream and transcoding it into a plurality of encodings, where each encoding uses a different bit rate. In one embodiment, default encoding parameters are provided in a configuration file. In another embodiment, default encoding parameters are provided at invocation. In one embodiment, individual source files may override default encoding parameters via an accompanying configuration file. In another embodiment, individual source files may override default encoding parameters using parameters provided at invocation. The R/S server 102 writes the transcoded data into segments then uploads the segments to the storage device 104. In one embodiment the recoding and segmentation may be invoked manually. In another embodiment, the recording and segmentation may be asynchronously invoked programmatically, based on pre-scheduled live events. The R/S server 102 is also responsible for segment encryption. In one embodiment, segments are encrypted before being uploaded to the storage device 104.

Figure 4 is a diagram 200 of the components of the R/S server 102. The live stream 212 is recorded by the stream recorder 202. The stream recorder 202 implements the specific protocol required to connect to the live stream 212. In one embodiment the protocol is RTMP. In another embodiment the protocol is RTSP/RTP. In another embodiment, the protocol is HTTP Live Streaming. In another embodiment, the protocol is MMS. There are numerous live streaming protocols, as should be known to those skilled in the art, of which any would be suitable for the stream recorder 202.

The stream recorder 202 passes recorded data to a stream transcoder 204 as it is received. The stream transcoder 204 is responsible for decoding the input stream and re-encoding the output video frames in the proper output codecs. The stream transcoder 204 passes the re-encoded frames to the output framer 206. The output framer 206 is

responsible for packing the encoded frames into the proper container format. In one embodiment, the stream transcoder 204 and output framer 206 support the H.264 , H263, MPEG2, MPEG4, and WVM, video codecs and the MP3, AAC, AMR, and WMA audio codecs, along with the FLV, MOV, 3GP, MPEG2-TS and ASF container formats. In another embodiment, the stream transcoder 204 and output framer 206 may support other standard or proprietary codecs and container formats. There are numerous video and audio codecs and container formats, as should be known to those skilled in the art, of which any would be suitable for the stream transcoder 204 and output framer 206. In one embodiment, the output framer 206 also supports the proprietary container format shown in Figure 5 and discussed below.

The output framer 206 writes the formatted data into segment files in the media storage 216. The output framer 206 is responsible for enforcing segment boundaries and durations. When the segments are complete, the output framer 206 notifies the segment encryptor 208. If segment encryption is required, the segment encryptor 208 reads the segment from the media storage 216, encrypts the segment, writes the encrypted segment back out to the media storage 216, and notifies the segment uploader 210 that the segment is ready for upload to the storage device 104. If no encryption is required, the segment encryptor 208 just notifies the segment uploader 210 that the segment is ready for upload to the storage device 104.

The segment uploader 210 uploads the finished segments to the storage device 104 (Figure 3). In one embodiment, the segment uploader 210 uses HTTP to upload segments. In another embodiment, segment uploader 210 uses FTP to upload segments. In another embodiment, segment uploader 210 uses SCP to upload segments. In another embodiment, segment uploader 210 uses simple file copy to upload segments. There are numerous methods, with varying levels of security, which may be used to upload the files, as should be known to those skilled in the art, of which any would be suitable for the segment uploader 210.

Figure 5 is a diagram 300 of a segment format which may be used in accordance with an embodiment of the present invention. The segment 302 contains a plurality of segment frames 304. Each segment frame 304 consists of a frame header 306 and a frame payload 308. The frame header 306 contains frame type information 310 and frame payload length information 312. In one embodiment, the frame type information 310 indicates the

payload track information (audio vs. video) as well as any additional information about the payload framing. The frame payload length 312 indicates the length of the segment frame payload 308 section. The frame payload length 312 may be used to parse the segment sequentially, without the need for global index headers and metadata to be packed at the beginning of the segment. In one embodiment, the frame header 306 is aligned to 4 or 8 byte boundaries to optimize copying of the frame payload 308.

The frame payload 308 contains further video frame encapsulation. In one embodiment, the encapsulation may be the further frame encapsulation may be for the RTP protocol. In another embodiment, the further frame encapsulation may be for the RTMP protocol. There are numerous video delivery protocols with different frame encapsulation formats, as should be known to those skilled in the art, which would be suitable for inclusion in the frame payload 308. In diagram 300, the further frame encapsulation shown is for the RTP protocol. The video frame is further encapsulated by the RTP packet header 314. The RTP payload 316 contains the actual video frame plus RTP padding 318. In one embodiment, RTP protocol padding 318 is used to pad the RTP payload 316 out to a 4 or 8 byte boundary, to ensure that the frame header 306 is 4 or 8 byte aligned, respectively. In another embodiment, custom padding may be added, outside of the protocol-specific frame encapsulation.

Figure 6 is a diagram 400 of a client device, wherein the client device native media player 410 supports RTSP/RTP for live streaming, which has been modified to support segment based live streaming, in accordance with an embodiment of the present invention.

In one embodiment, the client contains a downloader 402. The downloader 402 is responsible for interacting with the HTTP server 106 (Figure 3) to retrieve segments from the network storage device 104. The segments retrieved are written into the media buffer 420 and the downloader 402 notifies the segment decryptor 404. If the segment does not require decryption, the segment decryptor 404 notifies the segment parser 406 that the segment is ready. If the segment does require decryption, the segment decryptor 404 reads the segment from the media buffer 420, decrypts the segment, writes the decrypted segment back out to the media buffer 420, and notifies the segment parser 406 that the segment is ready.

RTSP requires separate frame based delivery for audio and video tracks. The RTP segments retrieved use the format 300 detailed in Figure 5. The segments are parsed by the

segment parser 406 to extract the individual audio and video RTP frames 308. The RTP frames 308 are already encapsulated for RTP simplifying the RTSP server 408. Once all the RTP frames 308 have been extracted and handed off to the RTSP server 408, the segment is no longer required. In one embodiment, the segment parser 406 removes the segment from the media buffer 420 once it has been completely parsed. In another embodiment, the segment parser 406 does not purge segments until the media buffer 420 is full. The RTSP server 408 handles requests from the media player 410 on the RTSP control channel 414, and manages setting up the audio and video RTP channels 416 and 418, and the audio and video RTCP channels 417 and 419. The audio and video RTP frames 308 are sent in a paced manner, by the RTSP server 408 on their respective RTP channels 416 and 418.

Figure 7 is a diagram 500 of a client device, wherein the client device native media player 510 supports HTTP Live Streaming, which has been modified to support segment based live streaming, in accordance with an embodiment of the present invention.

In one embodiment, the client contains a downloader 402. The downloader 402 is responsible for interacting with the HTTP server 106 (Figure 3) to retrieve segments. The segments retrieved are written into the media buffer 420 and the downloader 402 notifies the segment decryptor 404. If the segment does not require decryption, the segment decryptor 404 notifies the playlist generator 506 that the segment is ready. If the segment does require decryption, the segment decryptor 404 reads the segment from the media buffer 420, decrypts the segment, writes the decrypted segment back out to the media buffer 420, and notifies the playlist generator 506 that the segment is ready.

In the case of the HTTP Live Streaming client, MPEG2-TS format segments are retrieved. HTTP Live Streaming supports direct download of segments, as pointed to by an m3u8 playlist file. The playlist generator 506 is passed the file location, in the media buffer, by the segment decryptor 404. The playlist generator 506 updates the existing playlist adding the new segment and removing the oldest segment and passes the updated playlist to the HTTP server 508. The playlist generator 506 is also responsible for purging old segments from the media buffer 420. In one embodiment, segments are purged from the media buffer 420 as segments are removed from the playlist. In another embodiment, segments are only purged once the media buffer 420 is full, to support the largest possible rewind buffer.

The HTTP server 508 responds to playlist polling requests from the media player

510 with the current playlist provided by the playlist generator 506. The HTTP server 508 responds to segment requests from the media player 510 by retrieving the segment from the media buffer 420 and delivering it to the media player 510. The media player 510 connects to the HTTP server 508 though a local host HTTP connection 516.

For the clients in both Figure 6 and Figure 7, the downloader 402 is also responsible for calculating average available bandwidth. In one embodiment, the downloader 402 calculates the available bandwidth based on download time and size of each segment retrieved. In one embodiment, bit rate switching is initiated when the average available bandwidth falls below the current encoding's bit rate:

```
int bandwidth_avg      // average available network bandwidth
int video_bit_rate     // current video encoding bit rate

if bandwidth_avg < video_bit_rate
  for each encoding sorted by bit rate in descending order
    if encoding.bit_rate < bandwidth_avg && encoding.bit_rate != video_bit_rate
      change encoding
      break
    end
  end
end
```

The above can also be stated as, a bit rate switch is initiated when the download time required for a segment exceeds the duration of the segment. In one embodiment, a multiplier, less than one, is applied to detect network underruns before they occur:

```
int bandwidth_avg      // average available network bandwidth
int video_bit_rate     // current video encoding bit rate
int segment_download_time      // time to download most recent segment
int segment_duration           // duration of most recent segment
int multiplier                 // multiplier less than 1

if segment_download_time > segment_duration * multiplier
  for each encoding sorted by bit rate in descending order
    if encoding.bit_rate < bandwidth_avg && encoding.bit_rate != video_bit_rate
      change encoding
      break
    end
  end
end
```

In this scheme, the average network bandwidth is unable to sustain the video playout rate and a playback stoppage is imminent once the buffer runs out. This scheme requires relatively few calculations to determine when to switch encodings. However, it also has relatively low capability for predicting when a stoppage will occur. The encoding to switch to is the next lowest bit rate encoding whose bit rate is less than the average network bandwidth. Switching encodings to one of higher bit rate is initiated when the buffer occupancy of the media buffer 420 has reached its capacity and the average bandwidth exceeds the encoding bit rate of another encoding:

```
int bandwidth_avg       // average available network bandwidth
int video_bit_rate      // current video encoding bit rate
int buffer_occupancy    // seconds of video currently in the buffer
int buffer_capacity     // seconds of video the buffer can hold

if bandwidth_avg > video_bit_rate && buffer_occupancy >= buffer_capacity
  for each encoding sorted by bit rate in descending order
    if encoding.bit_rate < bandwidth_avg && encoding.bit_rate != video_bit_rate
      change encoding
      break
    end
  end
end
```

The encoding to switch to is the highest bit rate encoding whose bit rate is less than the average network bandwidth. This is an optimistic approach which assumes no further degradation in bit rate and works well when connected to a reliable, high bandwidth network. In another embodiment predictive bandwidth schemes may also be used to optimize rate adaptation for other environments.

Figures 8-10 are flow charts depicting various operations, and each is described in turn below. In these Figures, reference is made to various components of the system which are performing various steps of the operations. These components are shown in Figures 3-7 and are referred to below by the same reference numbers.

Figure 8 is a flow chart 600 describing the process of recording a live stream and creating the segments required for use in accordance with various embodiments of the present invention. In step 602, the stream recorder 202 begins retrieving and recording the live stream. In one embodiment, the live stream is delivered via a live streaming protocol such as RTMP, RTP, or Silverlight Smooth Streaming. In another embodiment, the live stream may be delivered via a near real-time streaming protocol such as HTTP Live Streaming. In another embodiment, the live stream may be read from pre-recorded video files. The stream recorder 202 buffers data in memory, and periodically writes the data to the stream transcoder 204, in step 604. The stream recorder 202 performs steps 602 and 604 in a continuous loop, for the duration of the live stream.

The stream transcoder 204 processing begins in step 606, once data has been queued by the stream recorder 202. In step 606, the stream transcoder 204 starts by decoding individual frames from the recorded data. In step 608, the stream transcoder 204 re-encodes each frame based on the output configuration. In step 610, the stream transcoder 204 passes the encoded frame to the output framer 206. In step 612, the stream transcoder 204 determines if additional encodings of the current frame are needed. If another encoding is

required, processing proceeds back to step 608 where the current frame is encoded into another encoding. If no additional encodings are required, processing proceeds back to step 606, where the next frame is decoded. In one embodiment, the stream transcoder supports generating a plurality of different bit rate encodings, as well as using a plurality of different codecs. The stream transcoder 204 encodes frames into a full permutation of bitrates and codecs. Steps 608, 610, and 612 are repeated for each encoding, on a given frame.

The output framer 206 processing begins in step 614 when frames are enqueued by the stream transcoder 204. The stream transcoder 204 produces multiple output frames for each input frame. In step 614, the output framer 206 maps each output frame to a specific output segment file, creating a new segment file in the media storage 216 if necessary. The output framer 206 synchronizes encoding configurations with unique segment files. In one embodiment, the output framer 206 also packs each frame into a plurality of segment file formats. In one embodiment, the frame formats include MPEG-TS and the custom frame format 300. In another embodiment, the frame format may include FLV or any other suitable container format, as should be known to those skilled in the art.

In step 616, the output framer 206 checks to see if the custom frame format for the RTP protocol 300 is required. If the custom frame format for the RTP protocol 300 is not required, then processing continues to step 620. If the custom frame format for the RTP protocol 300 is required, then processing proceeds to step 618 where the RTP packet headers 314, RTP padding 318, and the segment frame header 306 are added to the frame. The frame is then appended to the appropriate segment file, stored in the media storage 216, and processing continues to step 620. In one embodiment, only the custom format for the RTP protocol is required. In another embodiment, additional custom formats for RTMP or other protocols may be required. Steps 616 and 618 should be repeated for each additional custom frame format required.

In step 620, the output framer 206 checks to see if the MPEG-TS format is required. If the MPEG-TS format is not required, then processing continues to step 624. If the MPEG-TS format is required, then processing proceeds to step 622 where the frame and MPEG metadata headers are added to the appropriate segment file, stored in the media storage 216, and processing continues to step 624. In step 624, the output framer 206 checks to see if the segments are complete. In one embodiment, the segments are of a fixed duration, measured in seconds S. Given the constant frame rate R of the stream transcoder

204 output, the segments each contain a fixed number of frames F, where F = S * R. If the segment is not yet complete, processing proceeds back to step 614. If the segment(s) are complete, processing proceeds to step 626.

In step 626, the output framer performs any file post-processing. In one embodiment, file header reordering may be used to optimize the segment for client parsing. In another embodiment, additional hint tracks may be added to aid in client parsing. In another embodiment, additional compression may be applied to optimize segment delivery. Once the post-processing is complete, the output framer 206 notifies the segment encryptor 208 that the new segment(s) is available. The output framer 206 proceeds back to step 614, while the segment encryptor 208 proceeds to step 628.

In step 628, the segment encryptor 208 checks to see if encryption is required. If encryption is not required, processing continues to step 632. If encryption is required, processing continue to step 630 where the segment encryptor 208 reads the segment(s) from the media storage 218, encrypts the segment(s), and writes the segment(s) back out to the media storage 218, before continuing on to step 632. In step 632, the segment encryptor 208 notifies the segment uploader 210 that the new segment(s) is available. The segment encryptor 208 proceeds back to step 628 to wait for the next segment. The segment upload proceeds to step 634 where the segment is uploaded to the network storage 104.

Figure 9 is a flow chart 700 describing the process of delivering a live stream via HTTP to a client device 108 which supports RTSP. The process starts in step 702, when a user requests a video. The downloader 402 retrieves the first segment from the HTTP server 106 and signals the native RTSP media player 410 to initiate its RTSP connection to the RTSP server 408. The RTSP handshake and RTP port negotiation take place in parallel as the process continues to step 704. In step 704, the downloader 402 writes the segment to the media buffer 420 and notifies the segment decryptor 404 that a new segment is available. The downloader 402 proceeds to step 706, while the segment decryptor 404 proceeds to step 714.

In step 706, the downloader 402 checks to see if a bit rate change is required. Given the fixed segment duration of S seconds, download of live segments must take less than S seconds. If the download time for the previous segment exceeded some threshold T, where T < S, then a transition to a lower bit rate is required. If the download time for the previous segment was below a alternate threshold T', where T' << S, then a transition to a higher bit

rate may be required. In one embodiment, given three bit rate encodings, encoded at bitrates: B, B', B", where B < B' < B", the threshold T, for switching from B' to B, would be: T = C * S, where C is a constant multiplier and C < 1.0 (e.g. C = 0.8). In one embodiment, given three bit rate encodings, encoded at bitrates: B, B', B", where B < B' < B", the threshold T', for switching from B' to B" would be: T' = (C * S) * (B' / B") , where C is a constant multiplier and C < 1.0 (e.g. C = 0.8) and B' / B" represents the ratio of additional bandwidth required to support the new bit rate. In another embodiment, different thresholds may be used to favor upward or downward transitions. In deployments where high bandwidth and high network availability is expected, upward transitions may be favored. In deployments where network interruption is likely, downward transitions may be favored. In one embodiment, historical average segment download times are used to account for hysteresis. If the download time for the previous segment was between T' and T, then no action is needed, and processing continues to step 708. If a bit rate change is required, processing continues to step 708, where the new bit rate is chosen, then proceeds to step 710.

In step 710, the downloader 402 determines file name of the next segment. In one embodiment, the file names follow a well known naming convention such that bit rate and sequence number are embedded in the file name. In another embodiment, the file names may be retrieved from a Web service interface. The downloader 402 then begins polling for the next segment. In one embodiment, the downloader 402 calculates the time when the next segment will be available and waits until then to poll. In another embodiment, the downloader 402 may discount the segment availability time by the round trip delay for requesting the segment. In another embodiment, the downloader 402 begins polling immediately but uses an exponential decay algorithm to poll faster as the next segment availability time gets nearer. Once a new segment is retrieved, the downloader 402 returns to step 704.

In step 714, the segment decryptor 404 checks to see if the segment is encrypted. If the segment is not encrypted, then processing continues to step 718. If the segment is encrypted, processing continues to step 716, where the segment decryptor 404 reads in the segment from the media buffer 420, decrypts the segment, and writes the segment back out to the media buffer 420, then continues to step 718. In step 718, the segment decryptor 404 notifies the segment parser 406 that the new segment is available. The segment decryptor

404 returns to step 714, while the segment parser 406 proceeds to step 720.

In step 720, the segment parser 406 begins processing the custom segments 302 by extracting the next RTP packet 308. The custom segments 302 are parsed sequentially, using the payload lengths 312 to determine frame 304 boundaries. Each RTP packet 308 processed individually. The segment parser 406 queues the packet to the RTSP server 410, in step 722. In step 724, the segment parser 406 checks to see if the current frame is the last frame in the segment. If the current frame is not the last frame, the segment parser 406 proceeds back to step 720 to process the next frame. If the current frame is the last frame, the segment parser 406 proceeds to step 726 where it purges the segment, then continues back to step 720 to wait for the next segment. In one embodiment, segments are immediately purged by the segment parser 406. In another embodiment, the segment parser 406 waits until the media buffer 420 is full, before purging segments. If the mobile client 108 has limited memory immediate purging may be required, to make room for new segments in the media buffer 420. If the network is expected to have high error rates, immediate purging also frees up cache space in the media buffer 420, allowing more segments to be prefetched, which helps protect against future network errors. If the client application wishes to support rewind capabilities, delayed purging allows the media buffer 420 to cache previous segments for immediate access, when requested by the media player 410, rather than having to delay while the segment is re-downloaded.

The RTSP server 408 processes requests from the media player 410 asynchronously from the segment retrieval. Once the media player 410 negotiates the RTP connections 416 and 418 for the streaming session, the RTSP server 408 sends RTP packets 308 in a paced fashion, as dictated by timestamps in the RTP headers 314, as should be known to those skilled in the art. Step 728 shows the RTSP server 408 sending RTP packets to the media player 410. The RTSP server 408 maintains separate queues and separate timers for audio and video RTP packets to simplify parsing and delivery.

Figure 10 is a flow chart 800 describing the process of delivering a live stream via HTTP to a client device 108 which supports HTTP Live Streaming. The process starts in step 802, when a user requests a video. The downloader 402 retrieves the initial segments from the HTTP server 106 and signals the native HTTP Live Streaming media player 510 to initiate its HTTP connection to the HTTP server 508. In one embodiment, the m3u8 playlist requires multiple segments to be available to constitute a valid playlist. In one embodiment,

the downloader 402 downloads all the segments so that a valid m3u8 playlist may be generated for the initial media player 510 request. In another embodiment, only the first segment is downloaded and fake segments are used for the other segments, when generating the playlist. Processing then continues to step 804. In step 804, the downloader 402 writes the segment to the media buffer 420 and notifies the segment decryptor 404 that a new segment is available. The downloader 402 proceeds to step 806, while the segment decryptor 404 proceeds to step 814.

In step 806, the downloader 402 checks to see if a bit rate change is required. Given the fixed segment duration of S seconds, download of live segments must take less than S seconds. If the download time for the previous segment exceeded some threshold T, where $T < S$, then a transition to a lower bit rate is required. If the download time for the previous segment was below a alternate threshold T', where $T' << S$, then a transition to a higher bit rate may be required. In one embodiment, given three bit rate encodings, encoded at bitrates: B, B', B", where $B < B' < B''$, the threshold T, for switching from B' to B, would be: $T = C * S$, where C is a constant multiplier and $C < 1.0$ (e.g. $C = 0.8$). In one embodiment, given three bit rate encodings, encoded at bitrates: B, B', B", where $B < B' < B''$, the threshold T', for switching from B' to B" would be: $T' = (C * S) * (B' / B'')$, where C is a constant multiplier and $C < 1.0$ (e.g. $C = 0.8$) and B' / B'' represents the ratio of additional bandwidth required to support the new bit rate. In another embodiment, different thresholds may be used to favor upward or downward transitions. In deployments where high bandwidth and high network availability is expected, upward transitions may be favored. In deployments where network interruption is likely, downward transitions may be favored. In one embodiment, historical average segment download times are used to account for hysteresis. If the download time for the previous segment was between T' and T, then no action is needed, and processing continues to step 808. If a bit rate change is required, processing continues to step 806, where the new bit rate is chosen, then proceeds to step 808.

In step 808, the downloader 402 determines file name of the next segment. In one embodiment, the file names follow a well known naming convention such that bit rate and sequence number are embedded in the file name. In another embodiment, the file names may be retrieved from a Web service interface. The downloader 402 then begins polling for the next segment. In one embodiment, the downloader 402 calculates the time when the

next segment will be available and waits until then to poll. In another embodiment, the downloader 402 may discount the segment availability time by the round trip delay for requesting the segment. In another embodiment, the downloader 402 begins polling immediately but uses an exponential decay algorithm to poll faster as the next segment availability time gets nearer. Once a new segment is retrieved, the downloader 402 returns to step 804.

In step 814, the segment decryptor 404 checks to see if the segment is encrypted. If the segment is not encrypted, then processing continues to step 818. If the segment is encrypted, processing continues to step 816, where the segment decryptor 404 reads in the segment from the media buffer 420, decrypts the segment, and writes the segment back out to the media buffer 420, then continues to step 818. In step 818, the segment decryptor 404 notifies the playlist generator 506 that the new segment is available. The segment decryptor 404 returns to step 814, while the playlist generator 506 proceeds to step 820.

In step 820, the playlist generator 506 updates the current playlist adding the new segment and removing the oldest segment. Once segments have been removed from the playlist, the segments are no longer required in the media buffer 420. In one embodiment, segments are immediately purged by the playlist generator 506. In another embodiment, the playlist generator 506 waits until the media buffer 420 is full, before purging segments. If the mobile client 108 has limited memory immediate purging may be required, to make room for new segments in the media buffer 420. If the network is expected to have high error rates, immediate purging also frees up cache space in the media buffer 420, allowing more segments to be prefetched, which helps protect against future network errors. If the client application wishes to support rewind capabilities, delayed purging allows the media buffer 420 to cache previous segments for immediate access, when requested by the media player 510, rather than having to delay while the segment is re-downloaded.

The playlist generator 506 then notifies the HTTP Server 508 of the playlist update. Step 822 shows the HTTP server 508 getting the notification from the playlist generator 506, however, the HTTP server 508 processes requests from the media player 510 asynchronously from the segment retrieval. When the media player 510 requests playlists, the HTTP server 508 provides the most recent playlist made available by the playlist generator 506. When the media player 510 requests segments, the HTTP server 508 retrieves the segments from the media buffer 420 and returns them to the media player 510.

The media player 510 should only request segments that are in the playlist. The playlist generator 506 ensures that segments in the playlist exist in the media buffer 420.

In the description herein for embodiments of the present invention, numerous specific details are provided, such as examples of components and/or methods, to provide a thorough understanding of embodiments of the present invention. One skilled in the relevant art will recognize, however, that an embodiment of the invention can be practiced without one or more of the specific details, or with other apparatus, systems, assemblies, methods, components, materials, parts, and/or the like. In other instances, well-known structures, materials, or operations are not specifically shown or described in detail to avoid obscuring aspects of embodiments of the present invention.

CLAIMS

What is claimed is:

1. A live streaming system for delivering a live media stream to heterogeneous mobile endpoint devices, comprising:

a live streaming recorder operative to (1) capture the live media stream generated by a live media source and save the captured live media stream as a recorded stream in a recorded media file, and (2) transcode the recorded stream into a plurality of transcoded media files of respective different media encoding formats; and

a stream distribution subsystem operative to generate a plurality of distributed media streams each generated from one or more of the transcoded media files, each distributed media stream being delivered to a corresponding set of the mobile endpoint devices.

2. A live streaming system according to claim 1, wherein delivery of the distributed media streams to the mobile endpoint devices is via heterogeneous mobile providers.

3. A live streaming system according to any of claims 1 to 2, wherein time-shifted delivery of previous portions of the live media stream is made available to the mobile endpoint devices in near-real time.

4. A live streaming system according to claim 3, wherein the time-shifted delivery is made available in small chapterized video segments.

5. A live streaming system according to any one of claims 1 to 4, wherein the stream distribution subsystem includes a streaming tree having a root streamer and a plurality of streaming servers arranged in a hierarchical tree-topology, and wherein a media stream from the root streamer is relayed by the streaming servers to the mobile endpoint devices in a top-down hierarchical manner.

6. A live streaming system according to claim 5, wherein the streaming tree further includes a plurality of branch nodes interposed between the root streamer and the streaming servers, each branch node being operative to generate input media streams for corresponding

streaming servers from a corresponding media stream from the root streamer.

7. A live streaming system according to any of claims 1 to 6, wherein video and/or audio of the recorded stream is transcoded to a multiplicity of distinct formats.

8. A live streaming system according to any of claims 1 to 7, wherein delivery of each distributed media stream is via a delivery method selected from http-streaming, progressive download, RTSP, and full download.

9. A live streaming system according to any of claims 1 to 8, wherein a multiplicity of metadata associated with the live stream is created and stored in a database and made available to the mobile endpoint devices.

10. A live streaming system according to claim 9, wherein previously stored segments of video can be searched using the metadata stored in the database.

11. A live streaming system according to any of claims 1 to 10, wherein:

the live streaming recorder and transcoder are co-operative to (1) pack the plurality of transcoded media streams in a plurality of file formats each having formatted data, (2) write the formatted data out in segments, and (3) transfer the segments to a storage device accessible to a server; and

the stream distribution subsystem is operative to deliver the segments to the mobile endpoint devices sequentially for live media playback.

12. A method of delivering a live media stream to heterogeneous mobile endpoint devices, comprising:

capturing the live media stream generated by a live media source and saving the captured live media stream as a recorded stream in a recorded media file;

transcoding the recorded stream into a plurality of transcoded media files of respective different media encoding formats;

generating a plurality of distributed media streams each generated from one or more of the transcoded media files; and

delivering each distributed media stream to a corresponding set of the mobile endpoint devices.

13. A method according to claim 12, wherein delivery of the distributed media streams to the mobile endpoint devices is via heterogeneous mobile providers.

14. A method according to any of claims 12 to 13, wherein time-shifted delivery of previous portions of the live media stream is made available to the mobile endpoint devices in near-real time.

15. A method according to claim 14, wherein the time-shifted delivery is made available in small chapterized video segments.

16. A method according to any one of claims 12 to 15, utilizing a streaming tree having a root streamer and a plurality of streaming servers arranged in a hierarchical tree-topology, and wherein a media stream from the root streamer is relayed by the streaming servers to the mobile endpoint devices in a top-down hierarchical manner.

17. A method according to claim 16, wherein the streaming tree further includes a plurality of branch nodes interposed between the root streamer and the streaming servers, and further comprising, by each branch node, generating input media streams for corresponding streaming servers from a corresponding media stream from the root streamer.

18. A method according to any of claims 12 to 17, wherein video and/or audio of the recorded stream is transcoded to a multiplicity of distinct formats.

19. A method according to any of claims 12 to 18, wherein delivery of each distributed media stream is via a delivery method selected from http-streaming, progressive download, RTSP, and full download.

20. A method according to any of claims 12 to 19, wherein a multiplicity of metadata associated with the live stream is created and stored in a database and made available to the

mobile endpoint devices.

21. A method according to claim 20, wherein previously stored segments of video can be searched using the metadata stored in the database.

22. A method according to any of claims 12 to 21, further comprising:

packing the plurality of transcoded media streams in a plurality of file formats each having formatted data;

writing the formatted data out in segments;

transferring the segments to a storage device accessible to a server; and

delivering the segments to the mobile endpoint devices sequentially for live media playback.

23. A live streaming system for distributing live streaming data to client devices, comprising:

a processor for executing a live stream recorder and segmenter, wherein the live stream recorder accepts a live media stream and a configuration file;

a memory for storing output of the live stream recorder and segmenter; and

instructions executable by the processor for:

recording the live streaming data;

dynamically transcoding the live streaming data into a plurality of encodings;

packing the plurality of encodings in a plurality of file formats each having formatted data;

writing the formatted data out in segments;

transferring the segments to a storage device accessible to a server; and

delivering the segments to the client devices sequentially for live media playback.

24. A live streaming system according to claim 23, wherein the live streaming data includes audio and/or video data.

25. A live streaming system according to any of claims 23 to 24, wherein the live stream

data is transcoded into different formats for different types of client devices.

26. A live streaming system according to claim 25, further comprising transcoding each file format into different bit rates.

27. A live streaming system according to claim 25, further comprising adding custom frame headers to transcoded frames.

28. A live streaming system according to claim 27, wherein the custom frame headers include audio/video track information for each frame.

29. A live streaming system according to claim 27, wherein the custom frame headers include frame length information.

30. A live streaming system according to claim 27, wherein the custom frame headers include RTP packet headers.

31. A live streaming system according to any of claims 23 to 30, wherein each of the segments is of a predetermined fixed duration.

32. A live streaming system according to claim 31, wherein each segment duration is an integral number of seconds.

33. A live streaming system according to any of claims 23 to 30, wherein at least some of the segments are of variable durations.

34. A live streaming system according to claim 33, wherein all the variable segment durations are respective integral numbers of seconds.

35. A live streaming system according to any of claims 23 to 34, wherein the segments are encrypted before being transferred to the storage device.

36. A live streaming system according to any of claims 23 to 35, wherein the storage device is local to the segmenter.

37. A live streaming system according to any of claims 23 to 35, wherein the storage device is remote from the segmenter.

38. A live streaming system according to any of claims 23 to 35, wherein the storage device is accessible to an HTTP server, and wherein the segments are delivered to the client devices using the HTTP protocol.

39. A live streaming system according to any of claims 23 to 38, wherein delivery of the segments is via a delivery method selected from http-streaming, progressive download, RTSP, and full download.

40. A live streaming system according to any of claims 23 to 39, wherein a multiplicity of metadata associated with the live streaming data is created and stored in a database and made available to the client devices.

41. A live streaming system according to claim 40, wherein previously stored segments of video can be searched using the metadata stored in the database.

42. A method for distributing live streaming data to client devices, comprising:

recording the live streaming data;

dynamically transcoding the live streaming data into a plurality of encodings;

packing the plurality of encodings in a plurality of file formats each having formatted data;

writing the formatted data out in segments;

transferring the segments to a storage device accessible to a server; and

delivering the segments to the client devices sequentially for live media playback.

43. A method according to claim 42, wherein the live streaming data includes audio and/or video data.

44. A method according to any of claims 42 to 43, wherein the live stream data is transcoded into different formats for different types of client devices.

45. A method according to claim 44, further comprising transcoding each file format into different bit rates.

46. A method according to claim 44, further comprising adding custom frame headers to transcoded frames.

47. A method according to claim 46, wherein the custom frame headers include audio/video track information for each frame.

48. A method according to claim 46, wherein the custom frame headers include frame length information.

49. A method according to claim 46, wherein the custom frame headers include RTP packet headers.

50. A method according to any of claims 42 to 49, wherein each of the segments is of a predetermined fixed duration.

51. A method according to claim 50, wherein each segment duration is an integral number of seconds.

52. A method according to any of claims 42 to 49, wherein at least some of the segments are of variable durations.

53. A method according to claim 52, wherein all the variable segment durations are respective integral numbers of seconds.

54. A method according to any of claims 42 to 53, wherein the segments are encrypted

before being transferred to the storage device.

55. A method according to any of claims 42 to 54, wherein the storage device is local to a segmenter which performs the writing of the formatted data in segments.

56. A method according to any of claims 42 to 54, wherein the storage device is remote from a segmenter which performs the writing of the formatted data in segments.

57. A method according to any of claims 42 to 54, wherein the storage device is accessible to an HTTP server, and wherein the segments are delivered to the client devices using the HTTP protocol.

58. A method according to any of claims 42 to 57, wherein delivery of the segments is via a delivery method selected from http-streaming, progressive download, RTSP, and full download.

59. A method according to any of claims 42 to 58, wherein a multiplicity of metadata associated with the live streaming data is created and stored in a database and made available to the client devices.

60. A method according to claim 59, wherein previously stored segments of video can be searched using the metadata stored in the database.

61. Apparatus for retrieving live streaming data from a server, comprising:

a processor for executing a segment downloader and network proxy;

a memory for storing downloaded segments;

a rendering engine for rendering downloaded data, wherein the rendering engine communicates through the network proxy; and

instructions executable by the processor for:

measuring bandwidth at a client device;

selecting an appropriate bit rate for a current bandwidth in a delivery channel;

selecting an appropriate encoding for the client device; and

performing the following with respect to segments of the live streaming data: (1) requesting the segments from a server, (2) downloading the segments via the delivery channel, (3) storing the downloaded segments, (4) decrypting the stored segments, (5) parsing the decrypted segments, and (6) delivering the parsed segment data to a local media player through a local network proxy.

62. Apparatus according to claim 61, wherein the segments are requested and downloaded using the HTTP protocol.

63. Apparatus according to any of claims 61 to 62, wherein the stored segments are deleted upon delivery of the parsed segment data to the local media player.

64. Apparatus according to any of claims 61 to 62, wherein the stored segments are kept for a period of time after the parsed segment data is delivered to the local media player to support a rewind function.

65. Apparatus according to any of claims 61 to 64, wherein segment parsing includes decoding individual frames.

66. Apparatus according to any of claims 61 to 64, wherein segment parsing includes parsing file location information for use in generating playlists.

67. Apparatus according to any of claims 61 to 66, wherein the local network proxy is an HTTP server.

68. Apparatus according to any of claims 61 to 66, wherein the local network proxy is an RTSP server.

69. A method for retrieving live streaming data from a server, comprising:

measuring bandwidth at a client device;

selecting an appropriate bit rate for a current bandwidth in a delivery channel;

selecting an appropriate encoding for the client device; and

performing the following with respect to segments of the live streaming data: (1) requesting the segments from a server, (2) downloading the segments via the delivery channel, (3) storing the downloaded segments, (4) decrypting the stored segments, (5) parsing the decrypted segments, and (6) delivering the parsed segment data to a local media player through a local network proxy.

70. A method according to claim 69, wherein the segments are requested and downloaded using the HTTP protocol.

71. A method according to any of claims 69 to 70, wherein the stored segments are deleted upon delivery of the parsed segment data to the local media player.

72. A method according to any of claims 69 to 70, wherein the stored segments are kept for a period of time after the parsed segment data is delivered to the local media player to support a rewind function.

73. A method according to any of claims 69 to 72, wherein segment parsing includes decoding individual frames.

74. A method according to any of claims 69 to 73, wherein segment parsing includes parsing file location information for use in generating playlists.

75. A method according to any of claims 69 to 74, wherein the local network proxy is an HTTP server.

76. A method according to any of claims 69 to 74, wherein the local network proxy is an RTSP server.

77. An apparatus, comprising:

a processor for executing a live stream recorder and segmenter, wherein the recorder accepts a live media stream and a configuration file;

a memory for storing output of the live stream recorder and segmenter; and

instructions executable by the processor for:

recording the live media stream;

transcoding the recorded stream into a plurality of encodings as defined by the configuration file;

storing the encoded data in segments;

encrypting the plurality of resultant segments as defined by the configuration file; and

storing the transcoded and encrypted segments in the memory.

78. An apparatus, comprising:

a processor for executing a segment downloader and network proxy;

a memory for storing downloaded segments;

a rendering engine for rendering downloaded data, wherein the rendering engine communicates through the network proxy; and

instructions executable by the processor for:

connecting to a server to retrieve segments;

decrypting retrieved file data;

storing retrieved and decrypted segment data to the memory;

detecting a change in bandwidth that necessitates a change in bit rate and changing the bit rate at which future segments are retrieved;

parsing frames from the segment;

providing frames to the network proxy;

accepting connections to the network proxy from the rendering engine; and

streaming frame data to the rendering engine from the network proxy.

79. An apparatus, comprising:

a processor for executing a segment downloader and network proxy;

a memory for storing downloaded segments;

a rendering engine for rendering downloaded data, wherein the rendering engine communicates through the network proxy; and

instructions executable by the processor for:

connecting to a server to retrieve segments;

decrypting retrieved file data;

storing retrieved and decrypted segment data to the memory;

detecting a change in bandwidth that necessitates a change in bit rate and changing the bit rate at which future segments are retrieved;

generating a playlist file for the stored segments;

accepting connections to the network proxy from the rendering engine; and

sending playlist and segment data to the rendering engine from the network proxy.

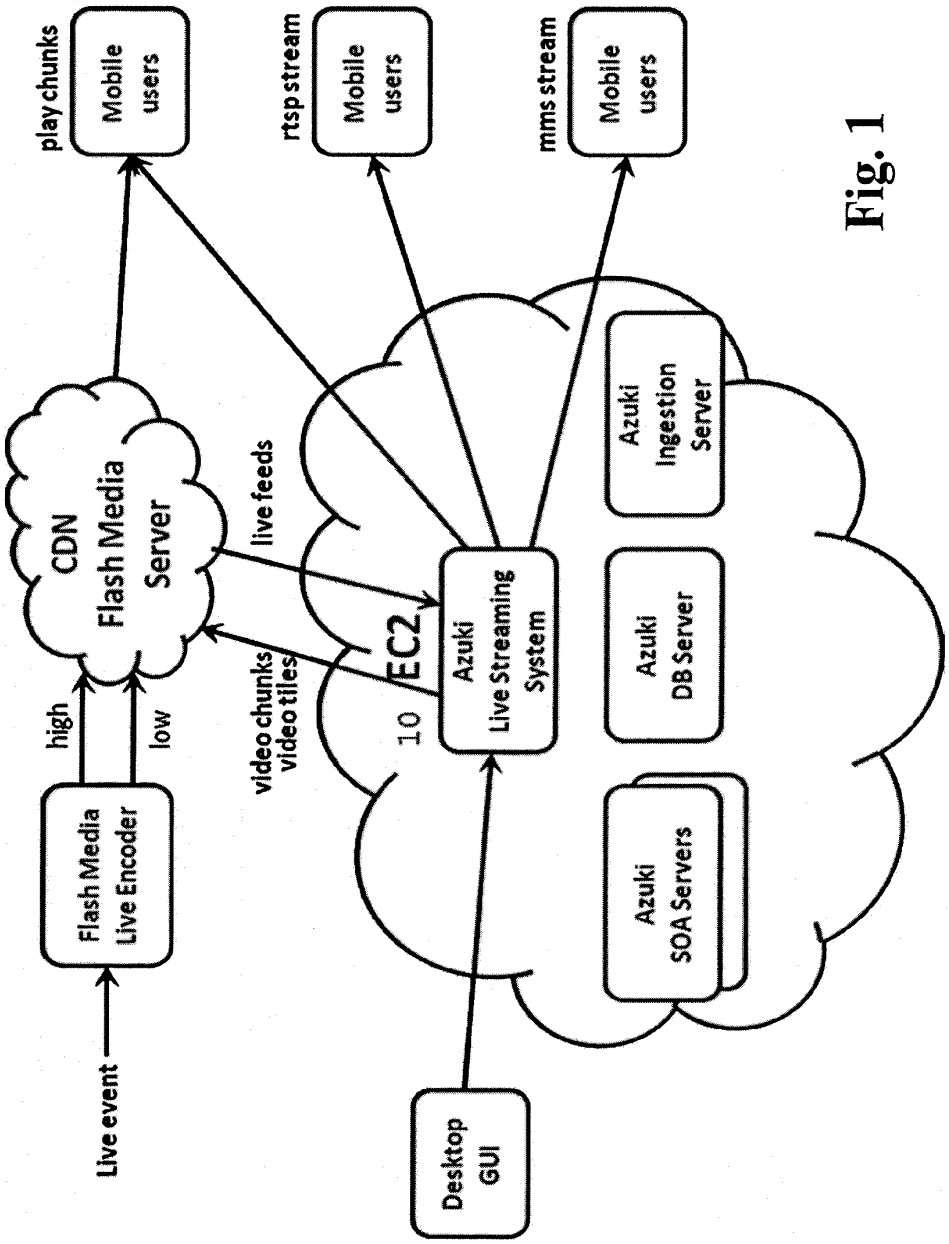

play chunks
Mobile users
rtsp stream
Mobile users
mms stream
Mobile users
CDN Flash Media Server
live feeds
video chunks video tiles
high
low
Flash Media Live Encoder
Live event
10
EC2
Azuki Live Streaming System
Azuki Ingestion Server
Azuki DB Server
Azuki SOA Servers
Desktop GUI

Fig. 1

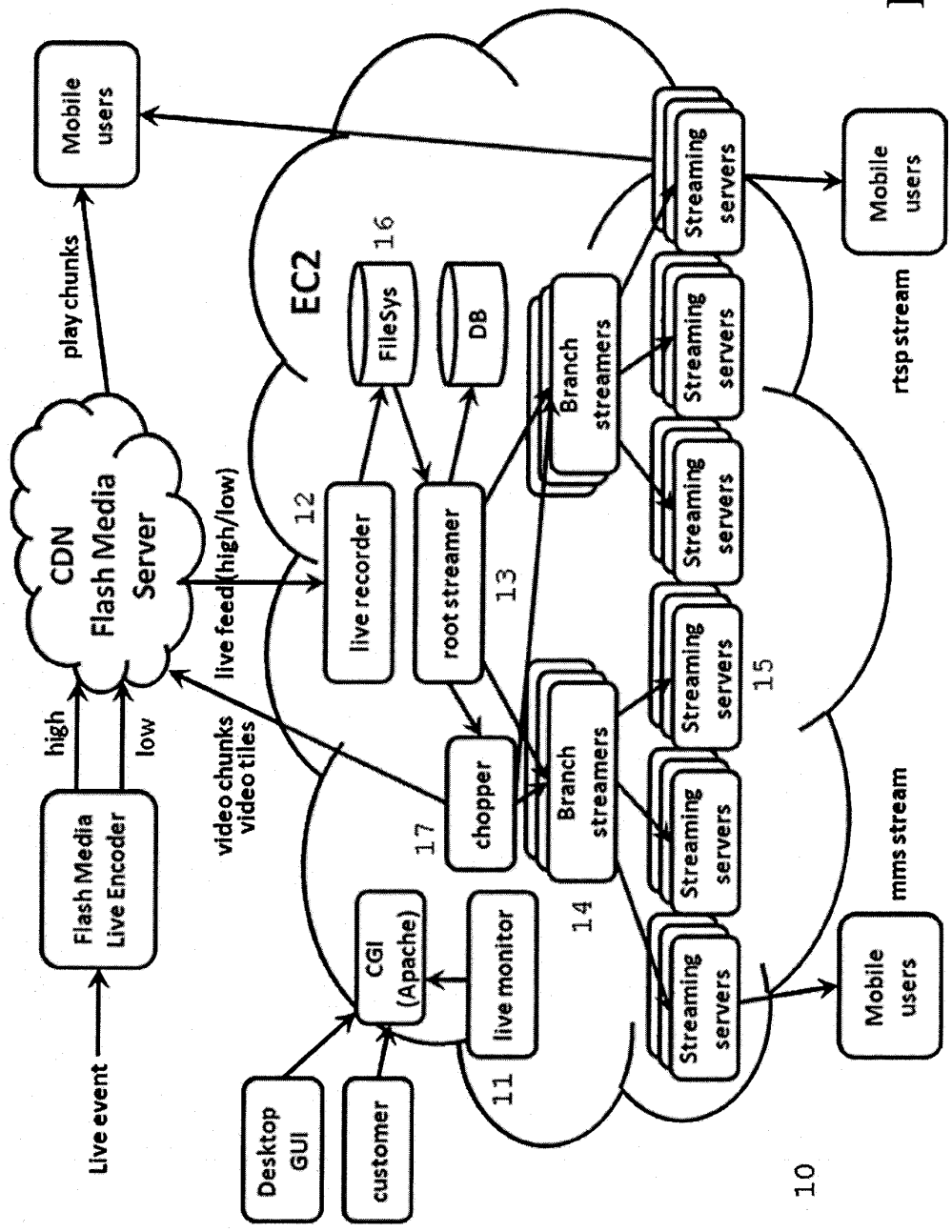

Live event
Flash Media Live Encoder
high
low
CDN Flash Media Server
play chunks
Mobile users
live feed (high/low)
video chunks video tiles
Desktop GUI
customer
CGI (Apache)
live monitor
11
EC2
12
live recorder
FileSys
16
DB
root streamer
13
chopper
17
Branch streamers
14
Streaming servers
15
rtsp stream
mms stream
10

Fig. 2

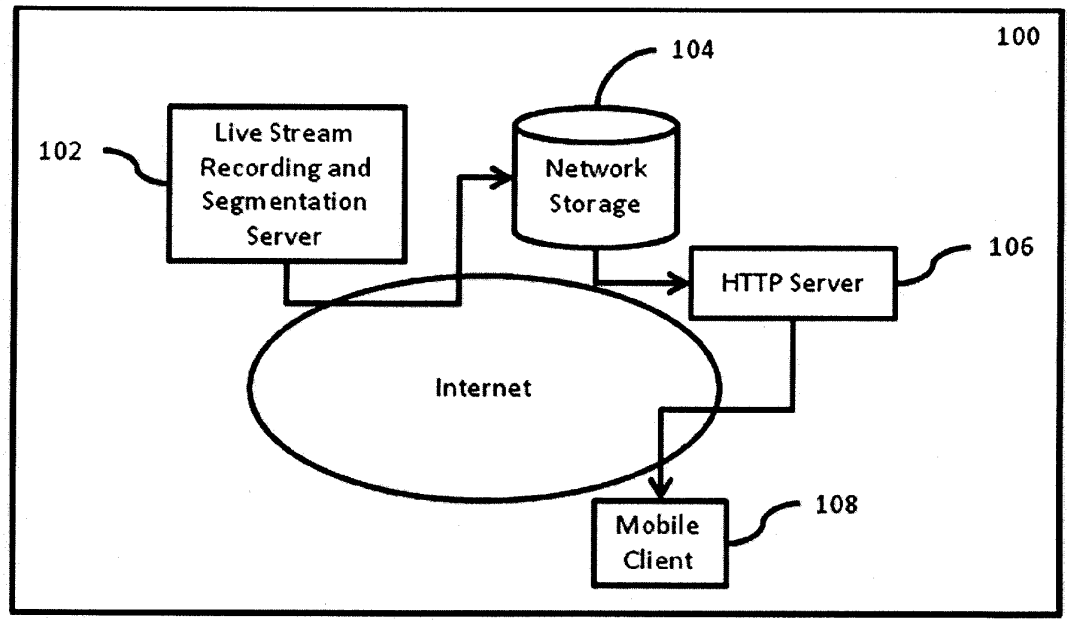

100
104
102
Live Stream Recording and Segmentation Server
Network Storage
106
HTTP Server
Internet
108
Mobile Client

Fig. 3

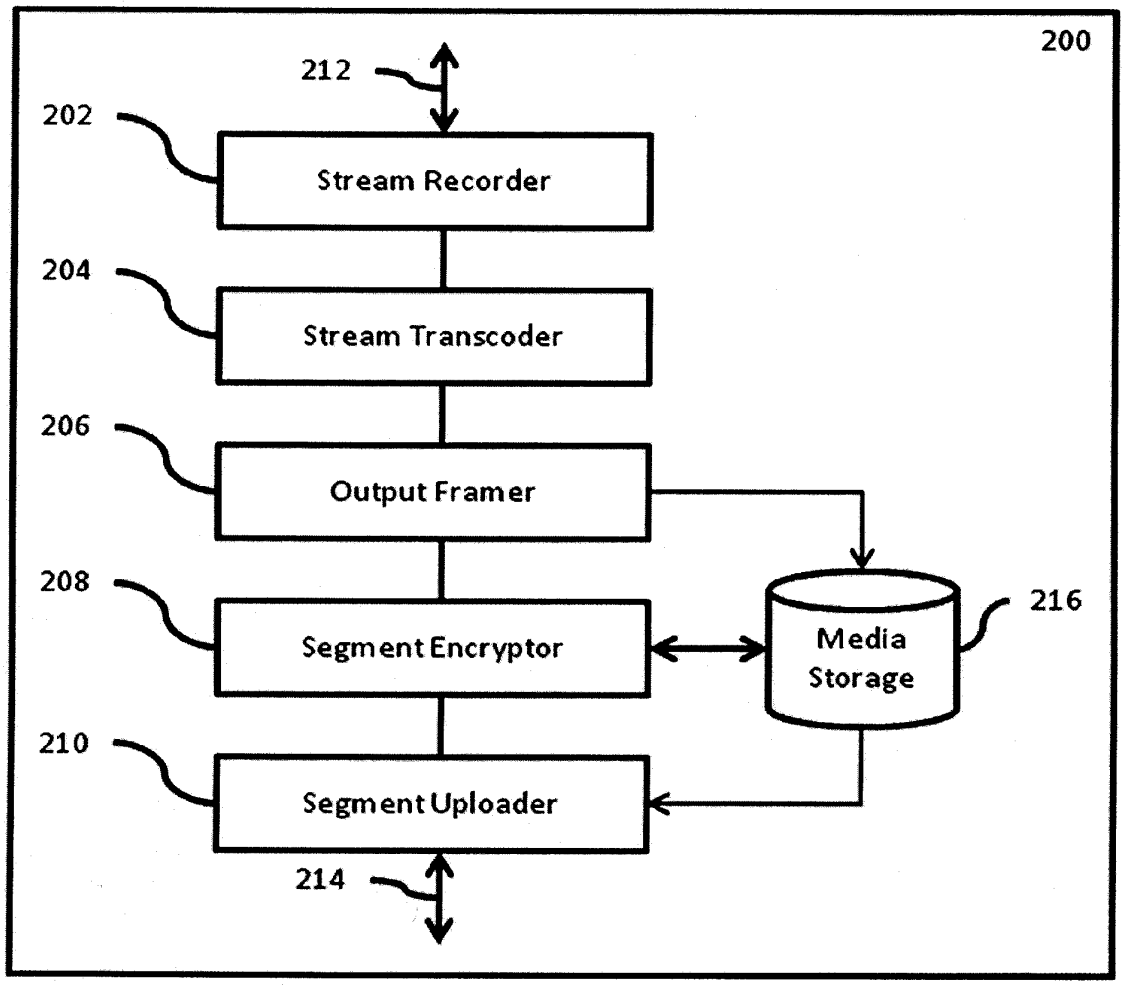

200
212
202
Stream Recorder
204
Stream Transcoder
206
Output Framer
208
Segment Encryptor
Media Storage
216
210
Segment Uploader
214

Fig. 4

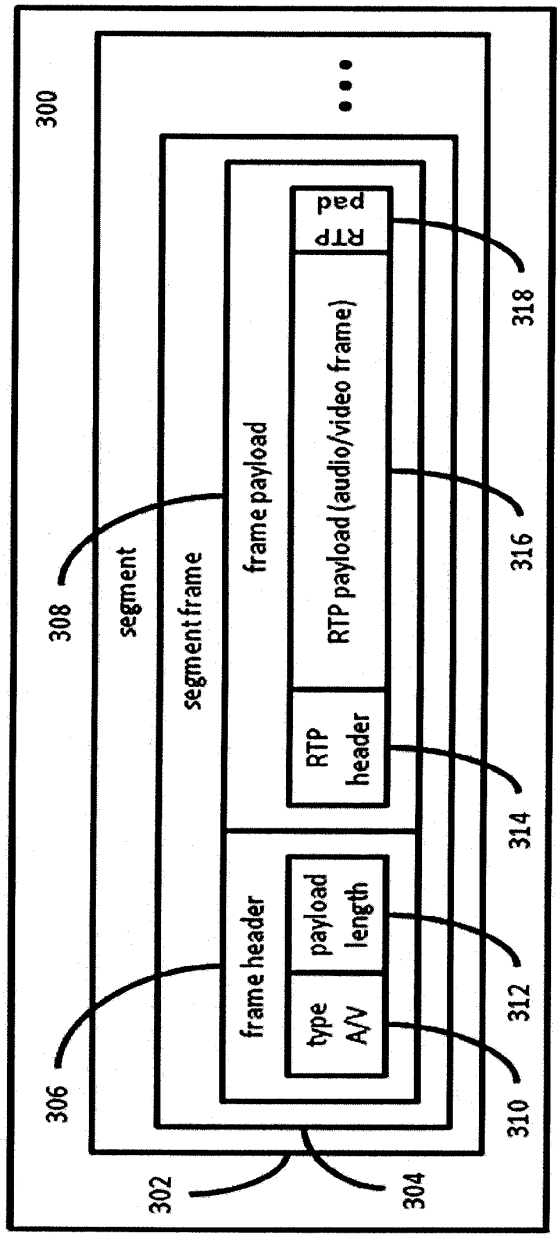


Fig. 5

EX1002 - Page 131

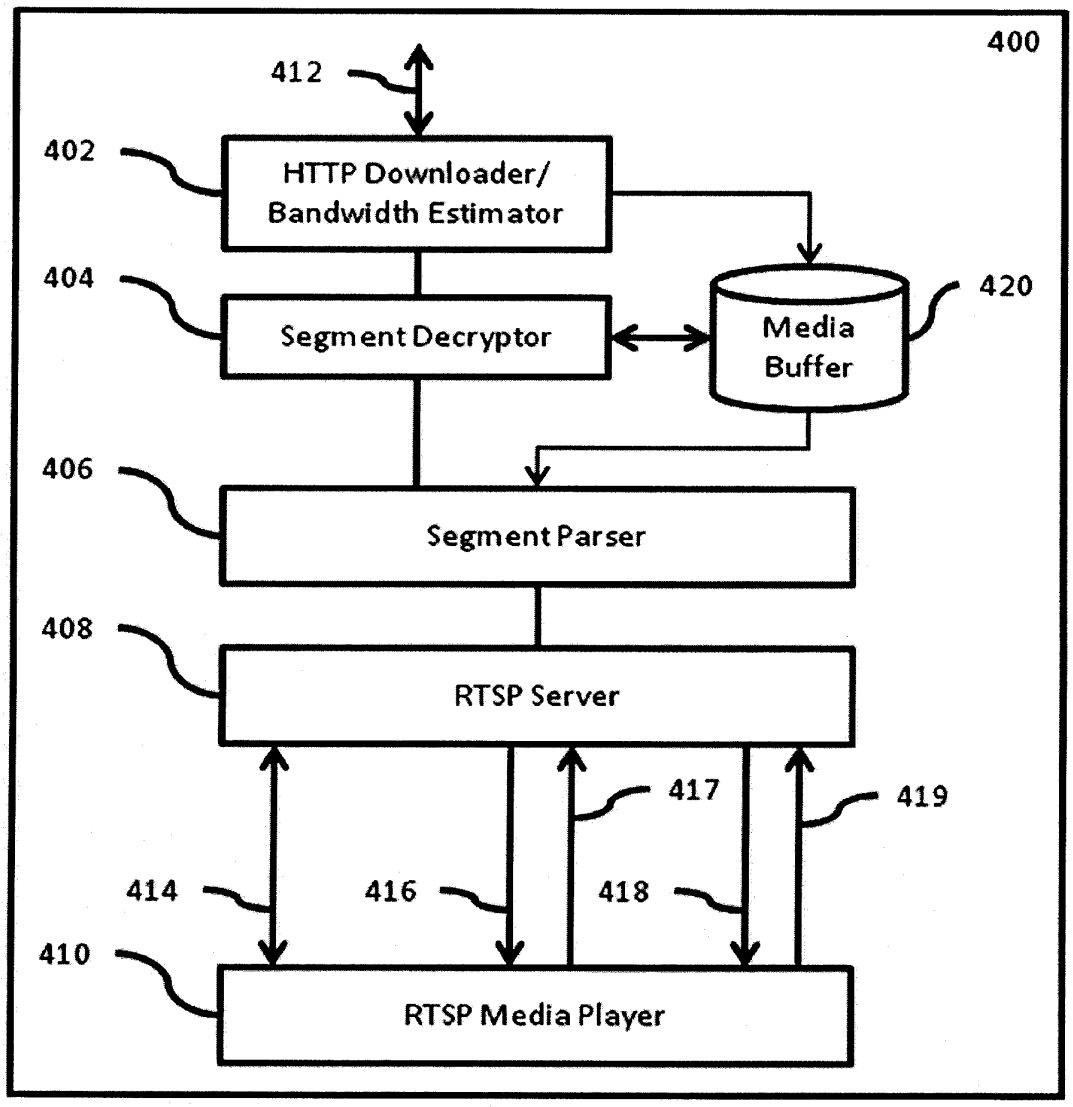

400
412
402
HTTP Downloader/
Bandwidth Estimator
404
Segment Decryptor
Media
Buffer
420
406
Segment Parser
408
RTSP Server
417
419
414
416
418
410
RTSP Media Player

Fig. 6

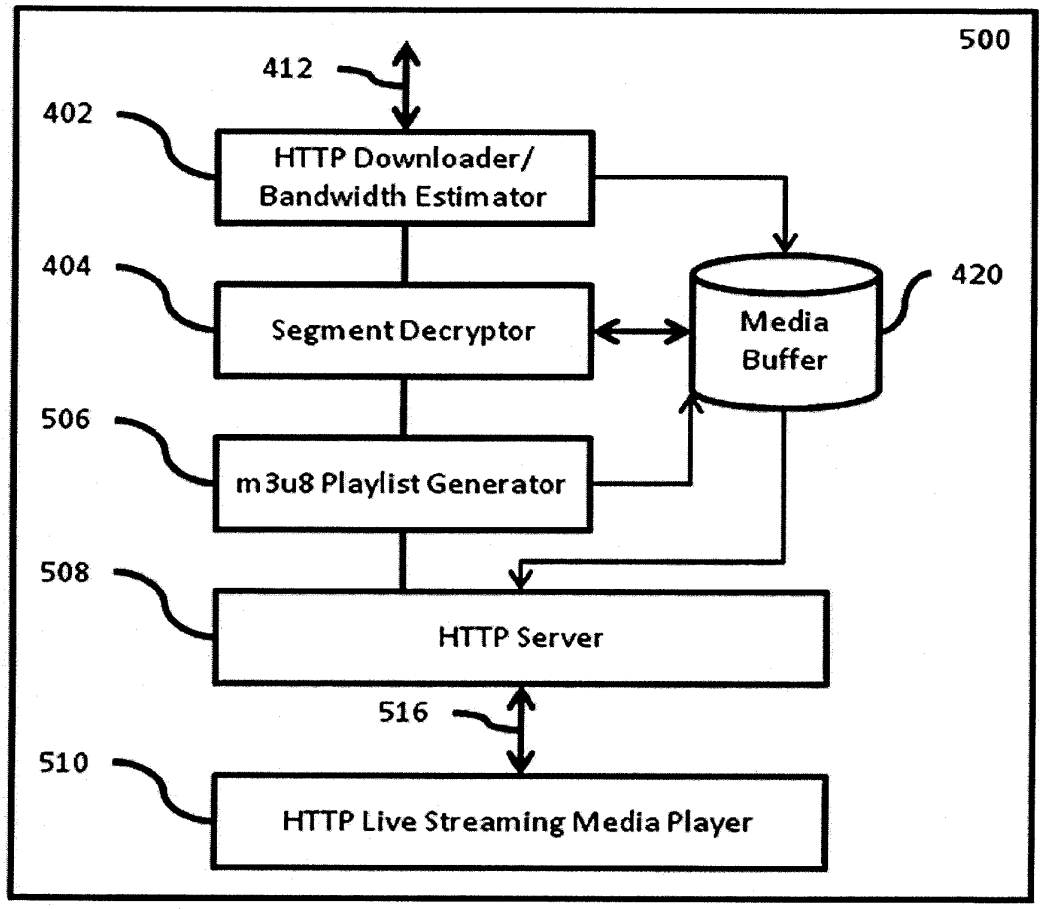

500
412
402
HTTP Downloader/
Bandwidth Estimator
404
Segment Decryptor
Media
Buffer
420
506
m3u8 Playlist Generator
508
HTTP Server
516
510
HTTP Live Streaming Media Player

Fig. 7

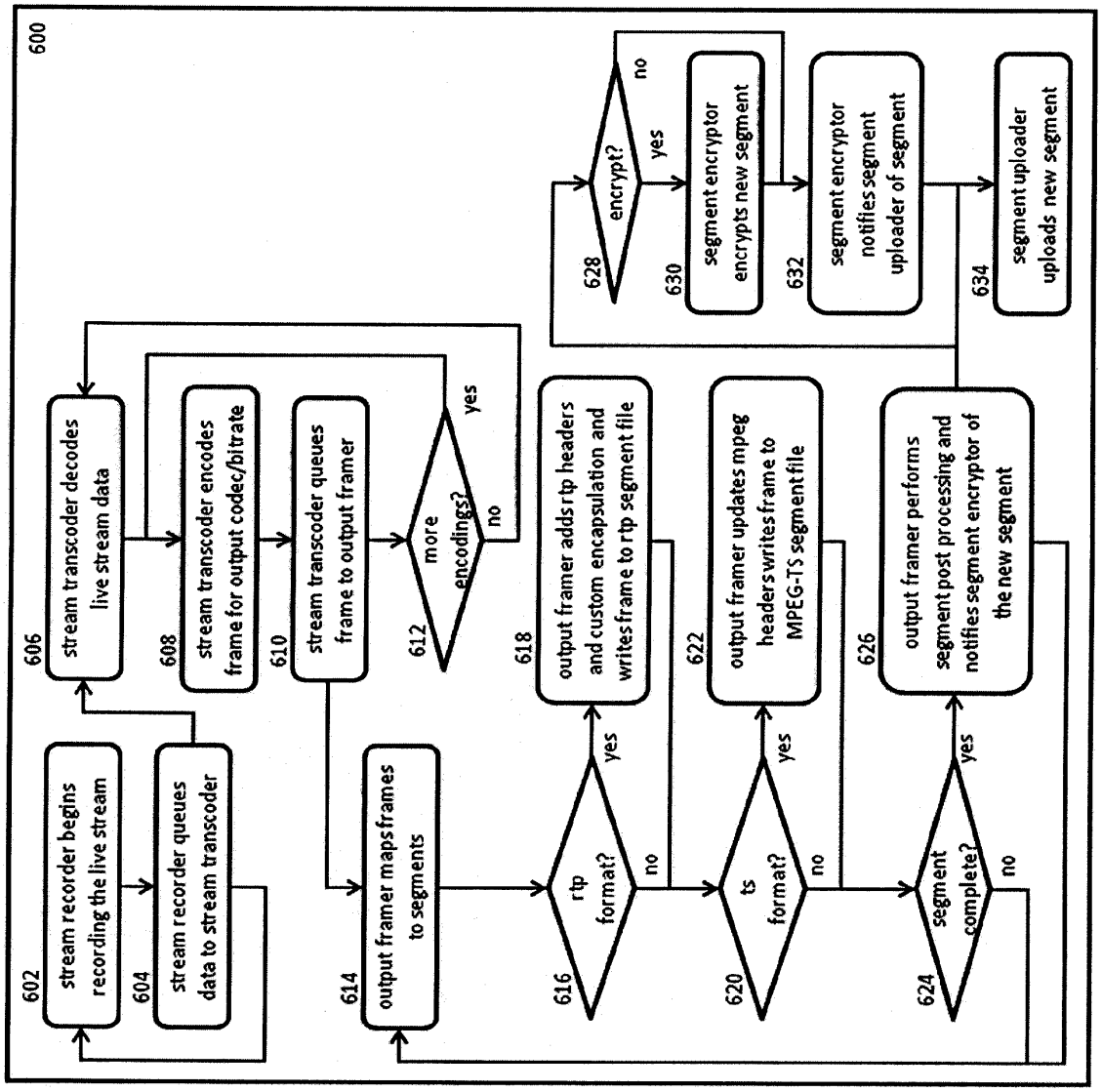

600
602
stream recorder begins recording the live stream
604
stream recorder queues data to stream transcoder
606
stream transcoder decodes live stream data
608
stream transcoder encodes frame for output codec/bitrate
610
stream transcoder queues frame to output framer
612
more encodings?
yes
no
614
output framer maps frames to segments
616
rtp format?
yes
no
618
output framer adds rtp headers and custom encapsulation and writes frame to rtp segment file
620
ts format?
yes
no
622
output framer updates mpeg headers writes frame to MPEG-TS segment file
624
segment complete?
yes
no
626
output framer performs segment post processing and notifies segment encryptor of the new segment
628
encrypt?
yes
no
630
segment encryptor encrypts new segment
632
segment encryptor notifies segment uploader of segment
634
segment uploader uploads new segment

Fig. 8

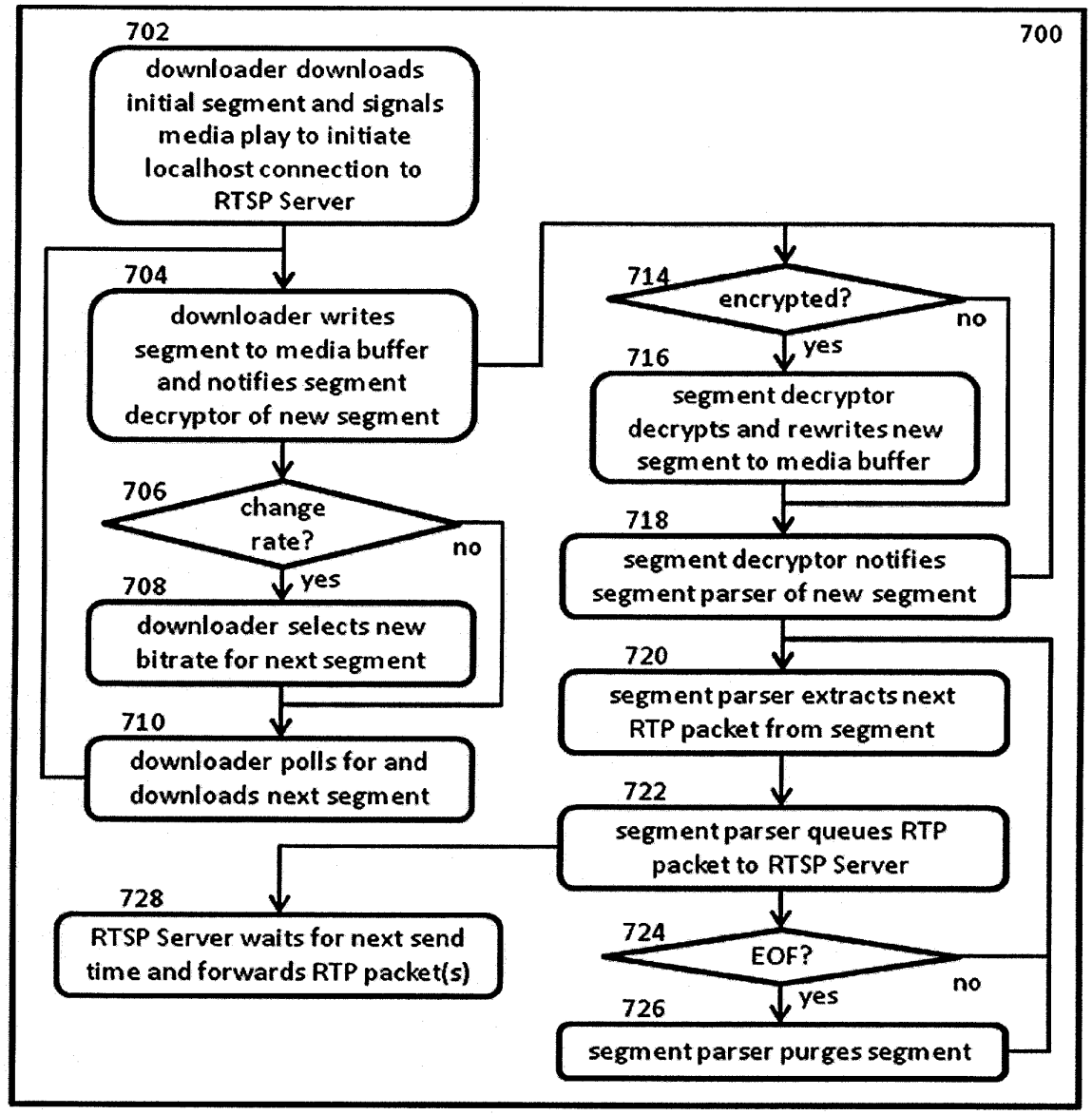

700
702
downloader downloads initial segment and signals media play to initiate localhost connection to RTSP Server
704
downloader writes segment to media buffer and notifies segment decryptor of new segment
706
change rate?
no
yes
708
downloader selects new bitrate for next segment
710
downloader polls for and downloads next segment
714
encrypted?
no
yes
716
segment decryptor decrypts and rewrites new segment to media buffer
718
segment decryptor notifies segment parser of new segment
720
segment parser extracts next RTP packet from segment
722
segment parser queues RTP packet to RTSP Server
724
EOF?
no
yes
726
segment parser purges segment
728
RTSP Server waits for next send time and forwards RTP packet(s)

Fig. 9

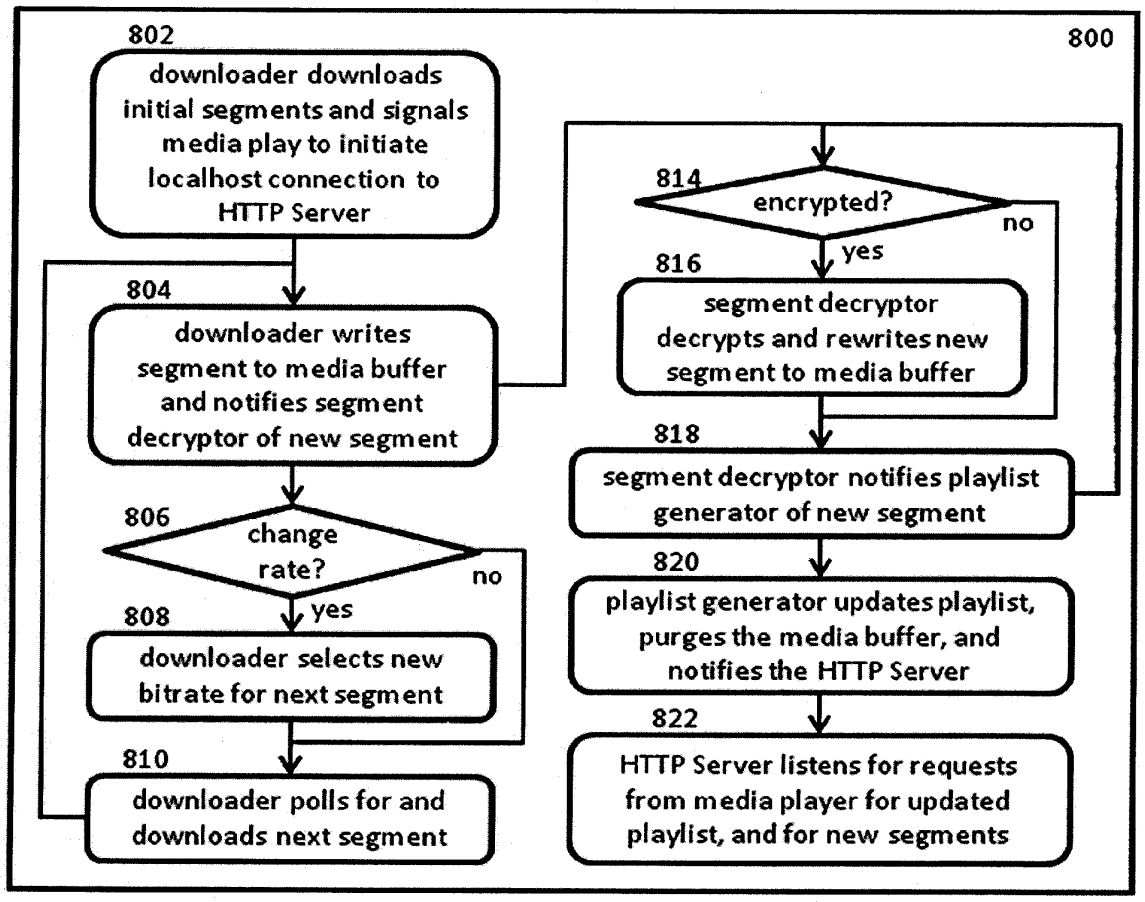

800
802
downloader downloads initial segments and signals media play to initiate localhost connection to HTTP Server
804
downloader writes segment to media buffer and notifies segment decryptor of new segment
806
change rate?
no
yes
808
downloader selects new bitrate for next segment
810
downloader polls for and downloads next segment
814
encrypted?
no
yes
816
segment decryptor decrypts and rewrites new segment to media buffer
818
segment decryptor notifies playlist generator of new segment
820
playlist generator updates playlist, purges the media buffer, and notifies the HTTP Server
822
HTTP Server listens for requests from media player for updated playlist, and for new segments

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 10/27893

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 15/16 (2010.01)
USPC - 709/231
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 709/231

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 709/203, 217, 231 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic databases: USPTO WEST (PGPB, USPT, EPAB, JPAB); Google Scholar
Search Terms Used: live or real time streaming, media or content or video, recording or recorder, encoding or transcoding, encrypting or decrypting, file or media formats, mobile or cellular or wireless, delivering or distributing, bit-rate or bandwidth

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0195746 A1 (Bowra et al.) 14 August 2008 (14.08.2008), entire document, especially; abstract, para [0008]-[0012], [0047]-[0070], [0079]-[0101])	1-4, 12-15, 23-30, 42-49, 61-64, 69-72, 77-79
Y	US 2004/0117427 A1 (Allen et al.) 17 June 2004 (17.06.2004), entire document, especially; abstract, para [0097]-[0111], [0468]-[0492], [0498]-[0525]	1-4, 12-15, 23-30, 42-49, 61-64, 69-72, 77-79
A	US 2008/0281977 A1 (Branam et al.) 13 November 2008 (13.11.2008), entire document	1-4, 12-15, 23-30, 42-49, 61-64, 69-72, 77-79
A	US 2007/0050828 A1 (Renzi et al.) 01 March 2007 (01.03.2007), entire document	1-4, 12-15, 23-30, 42-49, 61-64, 69-72, 77-79
A	US 2002/0023165 A1 (Lahr) 21 February 2002 (21.02.2002), entire document	1-4, 12-15, 23-30, 42-49, 61-64, 69-72, 77-79

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
26 April 2010 (26.04.2010)

Date of mailing of the international search report
30 APR 2010

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:
Lee W. Young
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 10/27893

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 5-11, 16-22, 31-41, 50-60, 65-68 and 73-76
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (2)) (July 2009)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 February 2011 (17.02.2011)

PCT

(10) International Publication Number
WO 2011/020088 A1

(51) International Patent Classification:
H04W 4/00 (2009.01)

(21) International Application Number:
PCT/US2010/045596

(22) International Filing Date:
16 August 2010 (16.08.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/234,092 14 August 2009 (14.08.2009) US

(71) Applicant *(for all designated States except US)*: **AZUKI SYSTEMS, INC.** [US/US]; 43 Nagog Park, Suite 105, Acton, MA 01720 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **NAIR, Raj** [US/US]; 6 Burroughs Road, Lexington, MA 02420 (US). **MIKHAILOV, Mikhail** [RU/US]; 183 Oak Street, Newton, MA 02464 (US).

(74) Agent: **THOMPSON, James, F.**; Bainwood, Huang & Associates, LLC, Highpoint Center, 2 Connector Road, Westborough, MA 01581 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR UNIFIED MOBILE CONTENT PROTECTION

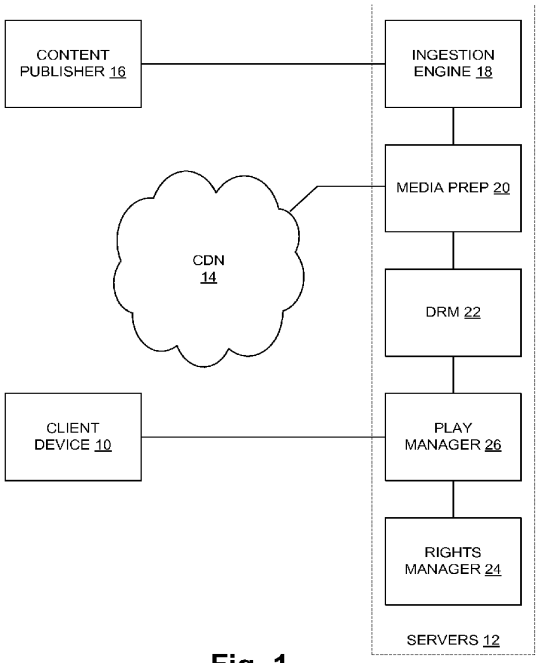


Fig. 1

(57) Abstract: Media content is delivered to a variety of mobile devices in a protected manner based on client-server architecture with a symmetric (private-key) encryption scheme. A media preparation server (MPS) encrypts media content and publishes and stores it on a content delivery server (CDS), such as a server in a content distribution network (CDN). Client devices can freely obtain the media content from the CDS and can also freely distribute the media content further. They cannot, however, play the content without first obtaining a decryption key and license. Access to decryption keys is via a centralized rights manager, providing a desired level of DRM control.

WO 2011/020088 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

METHOD AND SYSTEM FOR UNIFIED MOBILE CONTENT PROTECTION

BACKGROUND

The growing number of large form factor mobile devices such as the iPad has revolutionized mobile media consumption leading to revolutionary initiatives such as "TV Everywhere™" (TVE) with a mandate to make premium content available on a wide range of devices with great diversity in capabilities. This type of distribution, sometimes known as "Over-The-Top" (OTT) distribution, has underscored the need for a new and more robust trust model that builds on a 2-part trust model of user authentication and device identification and can offer the same level of content protection that content owners have had in the closed Consumer Electronics ecosystems of the past. The added level of protection can enable publishers to fully realize the potential for content distribution through this new open ecosystem of devices.

Content protection is challenging in mobile devices for a number of reasons. Mobile devices do not uniformly support Digital Rights Management (DRM) standards. In particular, most mobile devices do not currently support the most comprehensive form of content protection, the Open Mobile Alliance (OMA) V2.0 DRM standard. Mobile devices also vary in their CPU performance and memory capacity. An additional complication is the need to support multiple modes of delivery required in the mobile environment, such as live streaming, watching short video segments, rentals, or media download for watching later.

Current media protection schemes depend on sending the license information in-band with the media or using a pre-distributed license key in the media viewing device. Examples are Playready, WMDRM, Widevine, and Flash Access. However, TVE requires that the rights are transferable across devices in a seamless manner.

SUMMARY

The present invention relates in general to protecting media on mobile devices and more specifically to implementing a content protection system for media that may be streamed or watched offline on mobile devices. This system is particularly useful in the deployment of TVE services for protecting media on any Internet-connected device in an "Over-The-Top" (OTT) manner where the digital rights to the media are delivered to the device over the network and made specific to the device and user.

Methods and apparatus are disclosed for protecting content delivered to a variety of mobile devices based on client-server architecture with a symmetric (private-key) encryption scheme. In one embodiment, a media preparation server (MPS) encrypts all media content and publishes and stores it on a content delivery server (CDS), such as a server in a content distribution network (CDN). Clients can freely obtain media content from the CDS and can also freely distribute it further. They cannot, however, play the content without first obtaining a decryption key. Access to decryption keys is via a centralized rights manager, providing a desired level of DRM control.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages will be apparent from the following description of particular embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of various embodiments of the invention.

Figures 1 and 2 are block diagrams of systems capable of conducting procedures, in accordance with various embodiments of the invention;

Figure 3 is a diagram of the content encryption, in accordance with an embodiment of the present invention;

Figure 4 is a diagram of the key wrapping, in accordance with an embodiment of the present invention; and

Figure 5 is a block diagram of a system showing interfaces and message formats between system components;

Figures 6-8 are diagrams of message flows during system operation in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

Figure 1 is a block diagram for one embodiment of the present invention. It shows a client device 10 and a plurality of servers 12 that are connected together in a secure network and together form an instance of what is referred to herein as a "wireless platform" (WP). The client device 10 and WP servers 12 are typically computerized devices which include one or more processors, memory, storage (e.g., magnetic or flash memory storage), and

input/output circuitry all coupled together by one or more data buses, along with program instructions which are executed by the processor out of the memory to perform certain functions which are described herein. Part or all of the functions may be depicted by corresponding blocks in the drawings, and these should be understood to cover a computerized device programmed to perform the identified function.

In one embodiment, the servers 12 (referred to as servers herein) may be collocated in a single data center. In another embodiment, the servers 12 may be geographically distributed in multiple data centers. In another embodiment, the servers 12 may be physically in the same region, but connected to the client 10 through separate network paths (e.g. through different network service providers). In one embodiment, the servers 12 are situated as part of a content delivery network (CDN) 14. In one embodiment, the content from a content publisher 16 is ingested via an ingestion engine 18, and the ingested content is then segmented by a media preparation engine (MEDIA PREP) 20. The media preparation engine 20 obtains a content encryption/decryption key from a digital rights management (DRM) server 22 and uses it to encrypt the content for storage and later delivery in encrypted form. An example of streaming of content is shown in published PCT application WO 2010/045109.

In part of the description below, the combination of the ingestion engine 18, media prep 20 and a play manager 26 are referred to as a "content controller". Thus in one embodiment the system is constituted by a content controller along with a DRM server 22 and a rights manager 24.

A media preparation profile in the media preparation server 20 specifies an encryption type on a per-media-item basis. Candidate ciphers may include XOR, RC4, HC-128, AES, and along with the specification of encryption type is stored a corresponding key and a key length. Each media item has its own randomly generated key value. In the case of AES and XOR encryption, this randomly generated key value is used as the actual key for encryption/decryption, whereas for RC4 and HC-128 it is the seed key to initialize a stream cipher. AES key length is typically 128 bits. XOR key length may be 1024 bytes, and may be configurable. RC4 and HC-128 use 128 bit seed keys. The media preparation profile also specifies, on a per-media basis, the length of the byte stream which should be generated (this is the actual key used for media encryption, and the length is the same as the block length described elsewhere herein). Each media item is transcoded in multiple formats for different

target platforms, and each of the resulting transcoded media files is immediately encrypted with the chosen cipher and key and the encrypted files are then pushed to the CDN 14. Additional details regarding encryption are provided below.

In order to use the system for downloading content, the client device 10 first authenticates with the rights manager 24 and registers its device with the DRM server 20. During this process the client 10 obtains a logical device id from the rights manager 24 that is a token to represent a user of the client device 10, and associates this token with the specific client device 10 via a device "fingerprint" which is a unique identifier for the client device 10. The unique identification may be based on certain physical properties that may include an international mobile equipment identifier (IMEI) number, media access control (MAC) address, or certain file system properties. Each of the supported client devices 10 provides an Application Programming Interface (API) via which the unique identifier of that device can be obtained. Some devices have an IMEI number, some a mobile equipment identifier (MEID) number, some an electronic serial number (ESN). The iPhone has a unique device identifier (UDID).

The client device 10 has a built-in domain key that is used to encrypt the exchange of the logical device ID with the rights manager 24. For enhanced security, the domain key is divided into a number of separate components which are stored so as to be difficult to locate. For example, each may be stored as an array, with elements of the array represented as strings containing an integer and some special characters which are commonly found in binary files. When the arrays are examined, it is difficult to detect where the components are located. At run-time, all arrays are processed, special characters are discarded, and elements of these arrays are converted into characters and concatenated together to produce the actual domain key.

Device registration is carried out as follows. A DRM Agent running on the client 10 generates an encrypted token containing a device id and a randomly generated long nonce. That information (device id and the random long nonce) is encrypted with the domain key and is sent to the DRM server 22. The DRM server 22 decrypts this registration message using the same domain key, and stores an association between this user, device id, and key nonce in a database. The DRM server 22 generates a response containing a unique logical id assigned to this user. This response is encrypted with a session key constructed from domain key, device id, and the random key nonce provided by the DRM Agent, and the encrypted

response is sent to the client 10. Details regarding the construction of the session key are provided below.

Once the client 10 receives the response, it decrypts the response and stores registration information into an encrypted rights file on the client device 10. The rights file is encrypted with the key constructed from the combination of the domain key and the device id.

The session key may be constructed as follows:

A shared or domain key is combined with the device id and the randomly generated key nonce: shared_key + device_id + key_nonce. The resulting string is fairly long, so a hash or checksum is computed on it. In one embodiment, a hex representation of the hash, which may be 32 bytes long, is chosen to be the key. In different embodiments, the raw hash output (which may be a 128-bit integer) may be used. In one embodiment a Message Digest 5 (MD5) hash may be used. Other embodiments might use a 64-bit RACE Integrity Primitives Evaluation Message Digest (RIPEMD) hash function instead of MD5.

In other embodiments, it is possible to include other individualization parameters into these keys. Thus, the client/server session key, as well as the key used to encrypt the rights file on the device, could be enhanced further by adding unique user information (user token) and/or application information, such as the application name or identifier. That way, keys will be application-specific and user-specific as well as device-specific.

Figure 2 shows a slightly different embodiment of the system, in which there is a connection directly between the rights manager 24 and the DRM server 22 to enable the DRM server 22 to directly consult with the rights manager 24 as may be required.

As previously mentioned, any of various content encryption schemes may be employed. The following presents several specific examples along with corresponding details regarding how encryption/decryption is carried out. In some embodiments, the encryption can be applied to portions of the file such as key frames for video in order to reduce processing load.

<u>XOR</u>

In one embodiment the following simple and fast symmetric (private key) encryption scheme is used. Operation is illustrated in Figure 3. The media preparation server 20 performs an exclusive-OR operation (XOR) between the contents of the media file and a secret (private) key K1 (not shown). In one embodiment the key K1 is 1024 bytes long. The XOR

operation starts at a random position P1 within the media file and continues until the end of the file. The random position P1 is preferably chosen to be close to the beginning of the file, e.g. within the first 10% of the file. P1 can also be a predetermined fixed position, for example the very beginning of the file (location 0).

The key K1 may be chosen in a variety of ways. For example, it may be generated randomly. Alternatively, it may be generated by first choosing another random position P2 (not shown) within the same file, and selecting 1024 bytes from the media file starting at position P2. If there are not 1024 bytes remaining between P2 and the end of the file, then 1024 bytes are selected starting at position P2 – 1024 + 1. As noted, the key length may be other than 1024 bytes, and may be configurable.

The media preparation server 20 stores P1 and P2 in a database for each media file. In addition, the media preparation server 20 associates an expiration time with the encryption keys, stores the expiration time in the database, and re-encrypts content with new keys upon key expiration.

RC4-drop(n)

RC4-drop(n) is a stream-cipher algorithm generally known to those skilled in the art. It includes the dropping of the first 3072 bytes from each generated keystream. Also, RC4 does not have a formal notion of an initialization vector (IV). Instead, a checksum is computed on a concatenated key and an arbitrarily chosen initialization value, and the checksum is used as the key.

In one embodiment of stream cipher encoding, the entire media file is divided into smaller blocks of a selected block size. With a stream cipher, one can generate an infinitely-long stream of bytes. Theoretically, if a content item (e.g., movie) were to be played only from start to finish, without rewinding or fast-forwarding (i.e. without scrubbing), a stream cipher could be used on the streaming media without specialization. However, since the user may scrub during playback, decryption requires a modification to the stream cipher. The media is divided into fixed-size blocks and a new stream of key bytes is generated for each block by using the same seed key and a different IV. The IV in this case can be just the sequential block number, starting from 0. In one embodiment the blocks can have length 32k, but the block length can be different in other embodiments and may be configurable.

HC-128

HC-128 is another well-known stream cipher whose block size can be adapted as described above. Also, in addition to block size, both RC4 and HC-128 can take into account a segment number for live streaming and for video on demand (VOD). The entire long-form content is represented as many segments, and each segment is then divided into multiple blocks from the encryption/decryption point of view.

AES

The same approach to block sizing may be taken for AES unless of course in some embodiments the decryption is done in hardware. It may be desirable to use the same form of AES encryption supported by iPhone® and iPad®, which is AES bit with Cipher-Block-Chaining (CBC mode). Each segment is encrypted individually, and the same key is used across all segments, but each segment has its own initialization vector which is the sequence number of the segment.

It is briefly described how a user obtains a rights object (RO) to use in downloading and streaming, as well as playing, content. The user registers with a content provider using, in one embodiment, OpenID technology and obtains a user token which uniquely identifies that user. Before the user can play a given media content file, the user must obtain the decryption key. A DRM agent running on the client device 10 contacts the rights manager 24 and provides three items: <device-id, media-id, user-token>, where device-id is a unique identifier specific to that particular mobile device, media-id is a unique identifier specific to the particular media content the user wants to play, and user-token is the unique user identifier. Device id could be the unique address of the mobile device, or it may be one of the types of device identifiers discussed above.

The rights manager 24 receives the request for the RO from the client 10, containing <device-id, media-id, user-token>. The rights manager 24 validates the user-token using OpenID technology and also validates that media-id is correct and has not expired. It then generates the requested RO, which contains a key value K1 for media content decryption, a remaining play count for that media, and a media license expiration time. Even though communications between the client 10 and rights manager 24 is carried over a secure connection (SSL), the rights manager 24 may optionally encrypt the RO so that encrypted RO can be safely stored on the client device 10.

The encryption of the RO is illustrated in Figure 4. To encrypt the RO, the rights manager 24 uses the following symmetric encryption scheme. The RO is encrypted with 64-bit Blowfish key constructed from the checksum (domain key + device id + key nonce). To compute K2, the rights manager 24 applies an MD5 checksum function to the device-id.

Message Flow

Figure 5 contains a block diagram showing interfaces (numbered reference points) between system components. The following is a description of messaging flows (including message formats) among the components.

The ingestion flow consists of secure transfer of content from the content publisher 16 via a secure transfer method such as scp, sftp, or ascp (Aspera) to the content controller back-end server 28, which in turn transcodes and encrypts the content using the chosen content cipher (e.g., AES or HC-128) and publishes it into the CDN 14.

The interfaces and associated protocols are described next for each of the numbered reference points in Figure 5.

1. Over this HTTP interface, the client 10 performs a one-time device registration with the rights manager 24 (and DRM Server 22) passing the device-id, key nonce, and message nonce encrypted with the Blowfish algorithm using the domain key that is stored in an obfuscated manner in the application binary as described above. The registration information is passed through to the DRM Server 22 via the interface 2 described below. Depending on specific deployment requirements, the client may 10 may alternatively go to the DRM server 22 first, and the DRM server 22 then communicates with the rights manager 24.

Also, on the same interface, every time the client 10 needs to play a media, it sends media rights requests to the rights manager 24 also encrypted via Blowfish with a device-specific key. The media rights request contains device id, media id, logical id (a unique abstract user identifier) provided by the DRM server 24 when the device was registered, message nonce, and the current play count.

2. This HTTP interface is used as a pass-through interface, where the rights manager 24 relays requests (device registration and media location and rights requests) received from the client 10 and destined to the DRM server 22. These messages are encrypted as noted in #1. The rights manager 24 maintains user information which the DRM server 22 does not

have access to, and the rights manager 24 maps individual users to logical ids maintained by the DRM server 22. The rights manager 24 appends the logical id, uniquely identifying the current user, to all requests being forwarded to the DRM server 22. The only exception is the initial device registration because it does not have a logical id for that user at that point. The logical ids need not be encrypted when these servers are in a secure facility 30 with restricted access as shown. In environments where these servers need to be remote, a secure connection would be needed between them. The secure connection may take the form of a virtual private network (VPN) or a Secure Sockets Layer (SSL) connection.

3. This HTTP interface is used by the DRM server 22 to request media information from the back-end content controller 28. This interface is used to obtain information needed to play a media item. The request by itself does not have any commercial value and is therefore not encrypted nor sent over a secure channel.

4. This HTTP interface carries the response of the content controller 26 to the DRM server request described under item #3 above. The response is an XML document, containing media URL pointing to an encrypted media file located in the CDN 14 and an encrypted message which contains information about the cipher and the key used to encrypt this media. The message is encrypted with the Blowfish algorithm and the domain key.

5. Via this HTTP interface the DRM server 22 asks the rights manager 24 for media rights for the current user. The request contains logical id, media id, and the play count reported by the client 10. This interface is used when the client 10 is requesting media rights as described in #1. The information need not be encrypted when the DRM server 22 and rights manager 24 are in a secure facility 30. Alternatively, a secure connection may be employed.

6. This HTTP interface carries the response of rights manager 24 to the DRM server request described under item #5 above. The response is an XML document containing rights information for the requested media and the current user. This interface is used only when the client 10 is requesting media rights. The response need not be encrypted when the DRM server 22 and rights manager 24 are in a secure facility 30. Alternatively, a secure connection may be employed.

7. This HTTP interface sends the response of the DRM server 22 to the rights manager 24. Two types of responses are sent over this interface: the device registration response and the media location and rights in response to requests described under item #2

above.

The device registration response is an XML document that contains an encrypted message (containing the logical id) destined for the client 10, and also the logical id and total device count for the current user in the clear. The rights manager 24 uses the device count to check against the total count of authorized devices for the user. It removes the logical id and device count from the response, before forwarding it to the client 10 on interface 8. The client completes the registration on its end when it can receive the encrypted message and successfully decrypt and verify the nonce and checksum in the message.

The media rights and location response is an XML document that contains the media URL pointing to an encrypted media file located in a CDN 14, and an encrypted message (destined for the client) which contains information about the cipher and the key needed to decrypt this media and media rights information for the current user. This response is forwarded to the client 10.

In both types of responses, the message is encrypted with a key produced from the domain key, device id, and the key nonce.

8. This is a pass-through interface where the rights manager 24 simply forwards the responses it received from the DRM server 22 to the client 10, in response to the client's requests described under item #1 above. The contents of these responses are described fully in #7.

9. This is the interface by which the content is delivered to the client 10 from the CDN 14.

Figure 6 is a message flow ladder-diagram for one embodiment of the present invention. It describes the message flow for device registration and obtaining the rights object containing the content key for playing the content. Figure 7 contains another message flow ladder-diagram for an alternate embodiment where the client 10 is in direct communication with the intervening rights manager 24, which in turn communicates with DRM server 22.

Figure 8 illustrates a work flow for integrating functionality of a certificate authority (CA) into the content protection scheme. The work flow consists of the following steps:

1. Have a server certificate signed by the CA
2. Distribute the application to devices via application stores
3. Initially, a client 10 authenticates with a server via SSL via the following:

A. Authentication could be passed through to a customer authentication server 12

B. The customer authentication server 12 receives an activation code from the CA and passes it to the client 10

C. The client 10 uses the activation code (using tools of a software development kit (SDK) of the CA) to obtain an encrypted security credential from the CA, wherein the security credential = (the shared secret, a credential ID, and a creation time)

D. The client 10 sends the credential ID to the server 12 which is linked to an authentication record

E. The client 10 registers by sending the device fingerprint to the server 12 and gets a device-specific key

4. For a session, a client 10 is validated as follows:

A. The client uses the CA SDK to dynamically generate a security code from the security credential and sends it to the server 12 via SSL

B. The server 12 contacts the CA to validate the client 10 using the stored credential ID together with the security code

C. The server 12 returns the content key encrypted with the device-specific key

D. In offline mode, the DRM agent of the client 10 will offer protection with an offline timeout that forces contact with server 12 (which includes protection against clock tampering as described below)

Anti-Clock Rollback Protection

Clock rollback is a technique employed to illegally extend time-based licenses. A user manipulates the clock on a playback device so that the time-based license expiration is reached later than it should (or not at all). To detect clock roll-back, time is sampled on the client device 10 when the application is registered and every time it starts up, and the time is stored into the encrypted file. When a player is instantiated to play a media item, a separate thread is also started to monitor the progression of time during playback. The thread sleeps for a short time period, wakes up, and increments an elapsed time counter. That elapsed time is added to the last known local time. Thus, the application always has information about

what the time should be (to an approximation). This technique can be augmented to include time information from a server 12.

Rights File Integrity Protection

The rights file (also referred to as rights object herein) is stored on the client device 10 and contains the device-specific key and the content-keys encrypted with the device-specific key. The rights file itself is encrypted with the key constructed from the domain key and the unique identifier of the device. The contents of the file are checksummed and the checksum itself is stored within the file. When the file is decrypted, the contents are checksummed again and the computed checksum is compared with the checksum stored in the file to verify that the file has not been tempered with. The rights file also has a copy protection feature, in a sense that an outdated copy of the file cannot be written over the fresh copy without being detected by the DRM Agent. The copy protection is platform-dependent. On the iPhone/iPad platforms, DRM Agent obtains a unique property of the file and stores it within the encrypted file. The unique file value is not something that can be controlled at will, it is a property that is assigned by the operating system. Those skilled in the art may choose this file property such that copying the file would force a change in the unique value. On Android the rights file is stored within the application-specific directory which is protected from other applications and from user access via standard Linux permissions. Furthermore, DRM Agent generates a random long number and stores it within the encrypted file as well as within the application-specific directory on the device. The two numbers are compared when mobile application starts. On the Blackberry platform, a similar randomly generated long number is stored inside the encrypted file as well as within the application-specific persistent secure storage offered by the Blackberry platform.

In the description herein for embodiments of the present invention, numerous specific details are provided, such as examples of components and/or methods, to provide a thorough understanding of embodiments of the present invention. One skilled in the relevant art will recognize, however, that an embodiment of the invention can be practiced without one or more of the specific details, or with other apparatus, systems, assemblies, methods, components, materials, parts, and/or the like. In other instances, well-known structures, materials, or operations are not specifically shown or described in detail to avoid obscuring aspects of embodiments of the present invention.

Although the above description includes numerous specifics in the interest of a fully enabling teaching, it will be appreciated that the present invention can be realized in a variety of other manners and encompasses all implementations falling within the scope of the claims herein.

CLAIMS

What is claimed is:

1. A system for protecting media items delivered over the Internet to mobile devices wherein a license to each media item for a given mobile device is individualized to the given mobile device.

2. The system of claim 1 wherein the delivery is via segmented files over a hypertext transfer protocol.

3. The system of claims 1 or 2 wherein the license is also individualized to a specific user.

4. The system of claims 1 or 2 wherein the media item may have a plurality of representations for different bitrates.

5. The system of claim 4 wherein the player may switch arbitrarily between bitrates.

6. The system of claims 1 or 2 wherein the content is played offline.

7. A method for protecting content to be delivered to client devices via a content delivery network, comprising:

creating a media encryption key on a per-media basis during ingestion of media;

encrypting the media using the media encryption key;

pushing the encrypted media to the content delivery network for later delivery to client devices.

8. A method according to claim 7, further including per-media configuration of specific distinct encryption ciphers on a per-media basis.

9. A method according to claim 7 or 8, wherein the encryption ciphers include one or more stream ciphers for which a final key length is also per-media configurable.

10. A method according to claim 7, wherein encrypting the media uses one or more encryption ciphers selected from advanced encryption standard (AES), RC4, HC-128 and XOR.

11. A method according to claim 10, wherein encrypting the media includes performing an XOR operation using a key of a certain length L combined with data of protected content, the XOR operation comprising:

exclusive-OR'ing the key with L content bytes starting at a selected position of the content file;

exclusive-OR'ing the key with subsequent sets of L content bytes of the content file until all content bytes have been XOR'ed with the key.

12. A method according to claim 11, wherein the selected position is a predetermined position at or near a beginning of the content file.

13. A method according to claim 11, wherein the selected position in a beginning portion of the content file and chosen just prior to encrypting the content file.

14. A method according to claim 11, further including:

downloading an encrypted media item to a client device;

decrypting the encrypted media item only during playback and only in small quantities necessary for immediate playback, each small quantity spanning a range of content bytes determined by operation of a video player performing the playback and also by user scrubbing actions during playback, the scrubbing actions including rewinding and fast forwarding, the decrypting further including receiving a byte range and an offset of a first byte in the byte range from the beginning of the encrypted , and computing a mapping between the key and content bytes which need to be decrypted.

15. A method according to claim 10, wherein encrypting the media includes performing an HC-128 operation using a key of a certain length combined with data of protected content, the HC-128 operation comprising:

initializing an HC-128 stream cipher algorithm and generating a stream of bytes of a

preconfigured length, the length being configured on a per-media basis, the initialization including setting the value of an initialization vector employed by the HC-128 stream cipher algorithm to zero;

for a first set of content bytes of the preconfigured length, exclusive-OR'ing the stream of bytes with the set of content bytes;

for subsequent sets of the content bytes, (1) incrementing the initialization vector, (2) re-initializing the HC-128 stream cipher algorithm with the incremented initialization vector, and (3) repeating the generating of the stream of bytes and the exclusive OR'ing the stream of bytes with the subsequent sets of content bytes until the entire content file is fully encrypted.

16. A method according to claim 15, further including:

downloading an encrypted media item to a client device;

decrypting the encrypted media item only during playback and only in small quantities immediately necessary for playback, each small quantity spanning a range of content bytes determined by operation of a video player performing the playback and also by user scrubbing actions during playback, the scrubbing actions including rewinding and fast forwarding, the decrypting further including (1) receiving a range of bytes located anywhere within the media item along with an offset from the beginning of the media item, (2) identifying one or more initialization vectors needed to decrypt the bytes, (3) initializing the HC-128 algorithm using one of the identified initialization vectors, (4) generates a key stream, (5) exclusive- OR'ing the key stream with the bytes, and (6) repeating the above steps (3), (4) and (5) using distinct other ones of the initialization vectors for subsequent ranges of content bytes as necessary until the media item is fully decrypted.

17. A method according to claim 10, wherein encrypting the media includes performing an RC4 operation using a key of a certain length combined with data of protected content, the RC4 operation comprising:

initializing an RC4 stream cipher algorithm and generating a stream of bytes of a preconfigured length, the length being configured on a per-media basis, the initialization including setting the value of an initialization vector employed by the RC4 stream cipher algorithm to zero;

for a first set of content bytes of the preconfigured length, exclusive-OR'ing the stream

of bytes with the set of content bytes;

for subsequent sets of the content bytes, (1) incrementing the initialization vector, (2) re-initializing the RC4 stream cipher algorithm with the incremented initialization vector, and (3) repeating the generating of the stream of bytes and the exclusive OR'ing the stream of bytes with the subsequent sets of content bytes until the entire content file is fully encrypted.

16. A method according to claim 15, further including:

downloading an encrypted media item to a client device;

decrypting the encrypted media item only during playback and only in small quantities immediately necessary for playback, each small quantity spanning a range of content bytes determined by operation of a video player performing the playback and also by user scrubbing actions during playback, the scrubbing actions including rewinding and fast forwarding, the decrypting further including (1) receiving a range of bytes located anywhere within the media item along with an offset from the beginning of the media item, (2) identifying one or more initialization vectors needed to decrypt the bytes, (3) initializing the RC4 algorithm using one of the identified initialization vectors, (4) generates a key stream, (5) exclusive- OR'ing the key stream with the bytes, and (6) repeating the above steps (3), (4) and (5) using distinct other ones of the initialization vectors for subsequent ranges of content bytes as necessary until the media item is fully decrypted.

17. A method according to claim 10, wherein encrypting the media includes performing an AES operation using a key of a certain length combined with data of protected content, the AES operation comprising:

randomly generating AES encryption keys on a per-media basis at the time of ingestion of the media;

representing the media as multiple segments having corresponding sequence numbers;

establishing distinct initialization vectors for the segments;

performing an AES encryption algorithm on each segment using the respective initialization vector, the AES encryption algorithm including cipher block chaining within each segment and not spanning multiple segments.

18. A method according to claim 17, further including:

downloading an encrypted media item to a client device;

decrypting the encrypted media item using a native player of the client device, the native player having access to a playlist specifying a content decryption key, the playlist being served from a local HTTP server executing on the client device, the key being delivered to the client device from a digital rights management server via an encrypted message.

19. A method for delivering protected content to a client device, comprising:

registering the client device;

obtaining the license for use of the protected content;

decrypting the protected content; and

playing the decrypted content using a player of the client device.

20. The method of claim 19, further including detecting clock roll-back by use of a DRM agent executing on the client device to:

monitor a local clock to ensure that a time reported by the local clock is continuously incrementing;

at a time of starting a playback application, sampling the time and comparing it to a last known time stored in an encrypted rights file on the client device; and

employing a separate thread which wakes up at regular intervals as playback proceeds and (1) keeps track of elapsed playback time, (2) adding the elapsed playback time to the previously sampled local time on the client device, and (3) writing the result to the encrypted file.

21. The method of claim 19, further including detecting content expiration by:

maintaining rights information including an expiration time and/or maximum play count in association with each media item, the right information being received from a digital rights management (DRM) server in an encrypted form, and storing the rights information in an encrypted file on the client device;

upon initiating playback of the media item, employing a DRM agent on the client device to determine whether the media item has expired by comparing a current time on the client device to the expiration time of the media, and/or comparing the maximum play count to a stored actual play count, the DRM Agent ensuring that clock rollbacks on the client

device are detected and disallowing media playback if time is not steadily incrementing, the DRM Agent executing a separate thread, in parallel with a thread performing playback such that the media item can expire not only upon initiating playback but also during playback.

22. The method of claim 19, further including

uniquely identifying the client device using a unique physical device identifier, the unique physical device identifier being obtained from the client device using an application programming interface offered by an execution environment of the client device, the unique physical device identifier being encrypted with a domain secret and stored in an encrypted file on the client device and also sent to a digital rights management (DRM) server via an encrypted message, the encrypted unique physical device identifier being stored by the DRM server in a database of registered client devices and being mapped to a unique logical device identifier representing a user of the client device, the unique logical device identifier being sent encrypted with the domain secret.

23. The method of claim 22, wherein the unique physical device identifier is selected from an IMEI number, an MEID, an ESN and a UDID.

24. The method of claim 22, further comprising:

combining the unique physical device identifier with a domain key to generate a device-specific key to encrypt a rights file stored on the client device and containing content decryption keys used to decrypt the protected content.

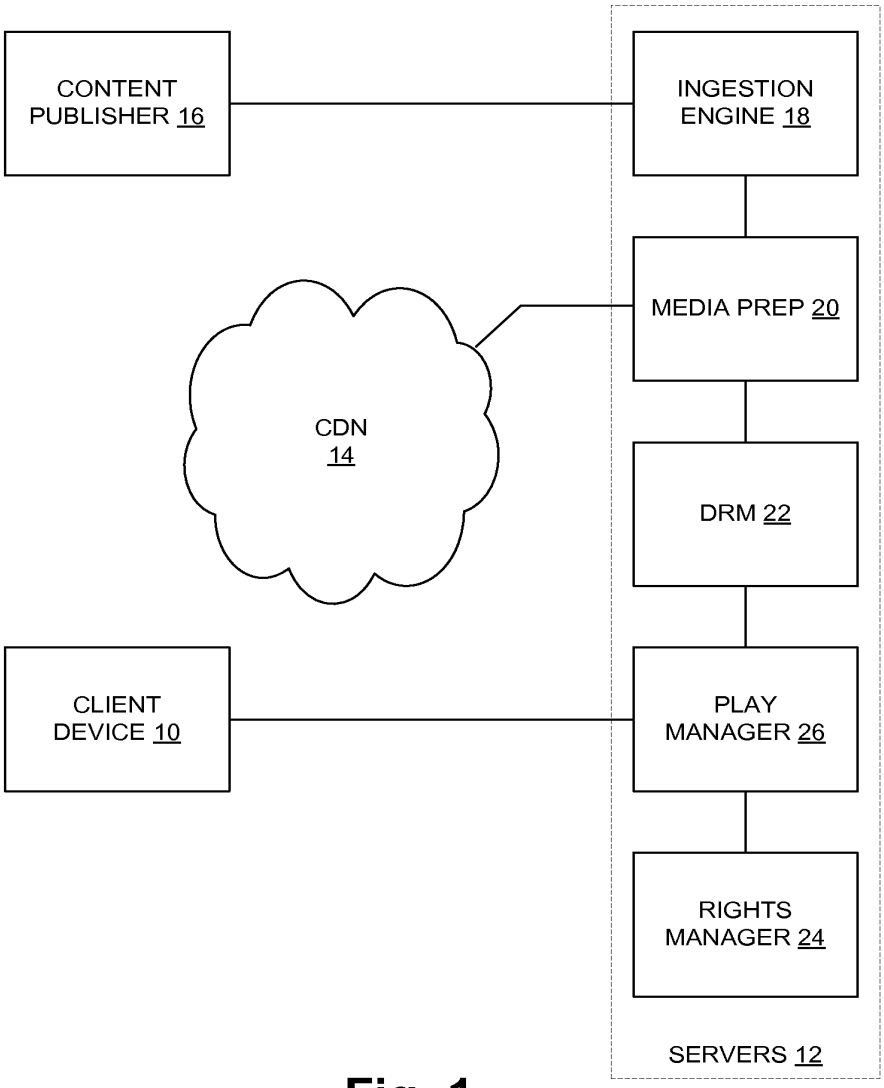

CONTENT PUBLISHER 16
INGESTION ENGINE 18
MEDIA PREP 20
CDN 14
DRM 22
CLIENT DEVICE 10
PLAY MANAGER 26
RIGHTS MANAGER 24
SERVERS 12

Fig. 1

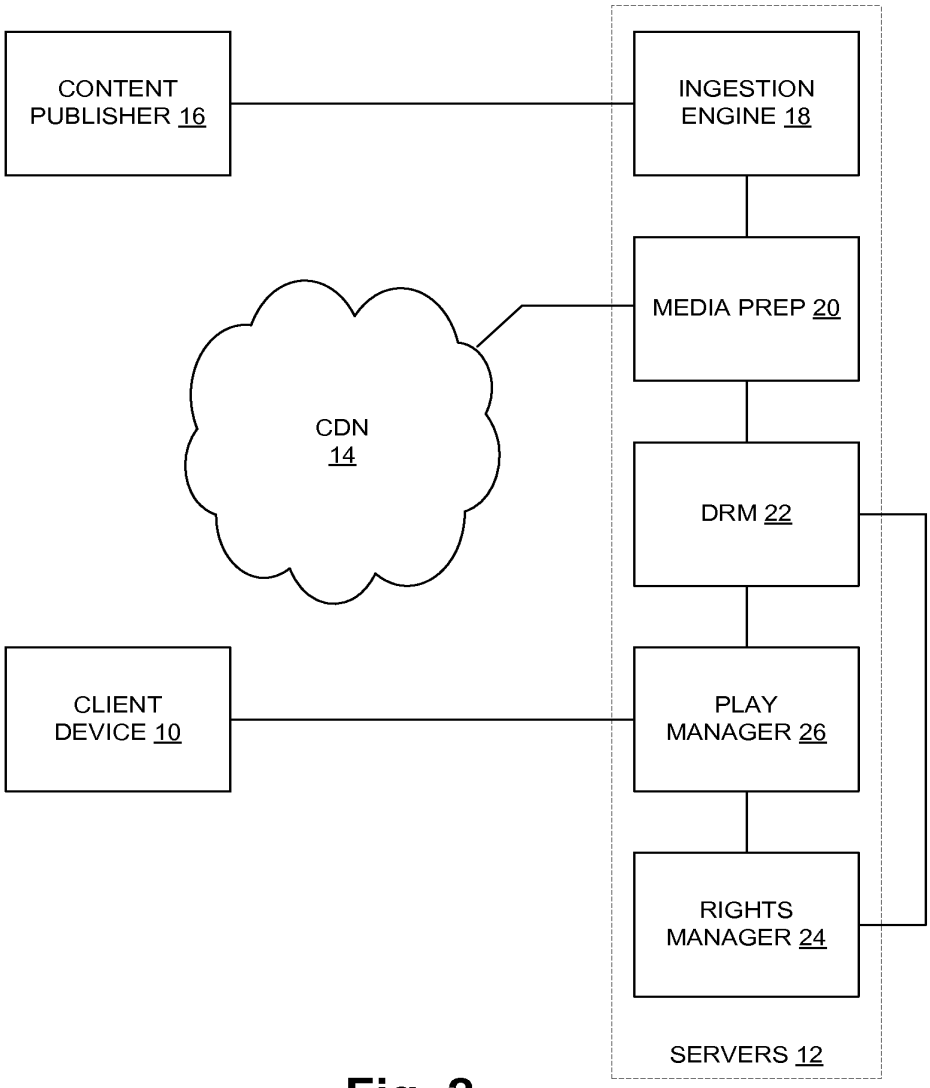

CONTENT PUBLISHER 16
INGESTION ENGINE 18
MEDIA PREP 20
CDN 14
DRM 22
CLIENT DEVICE 10
PLAY MANAGER 26
RIGHTS MANAGER 24
SERVERS 12

Fig. 2

Fig. 3

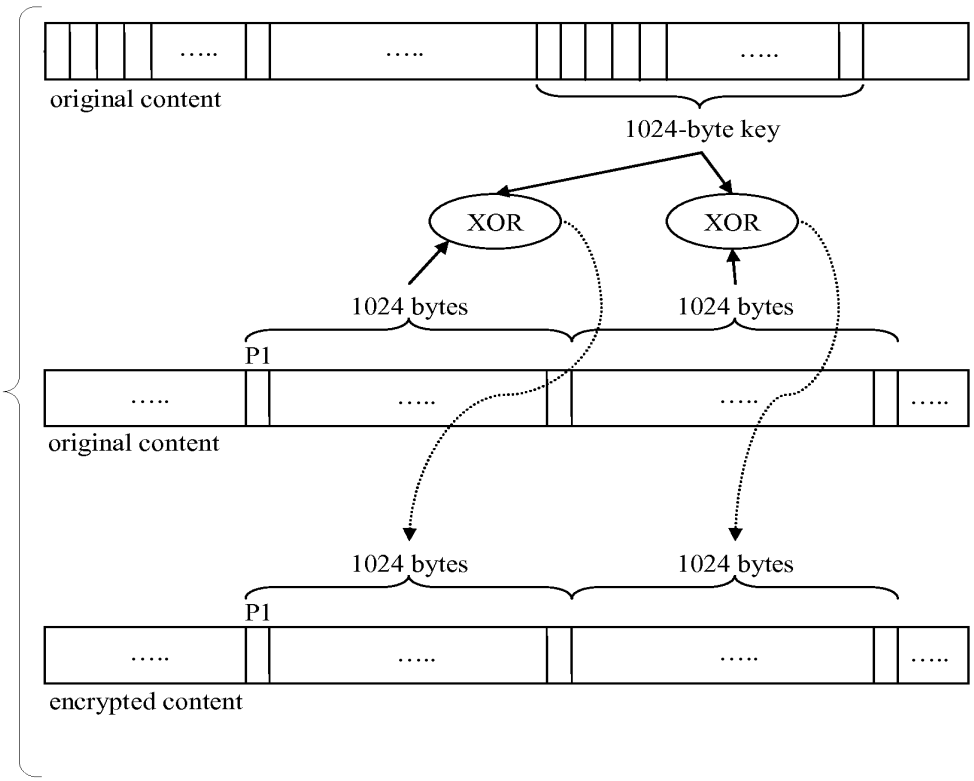
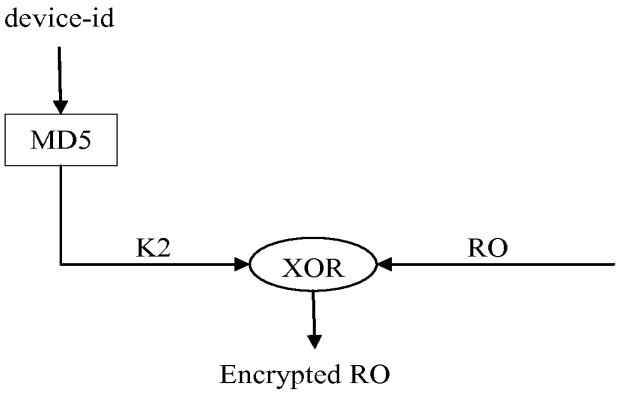

original content
1024-byte key
XOR
XOR
1024 bytes
1024 bytes
P1
original content
1024 bytes
1024 bytes
P1
encrypted content

Fig. 4


device-id
MD5
K2
XOR
RO
Encrypted RO

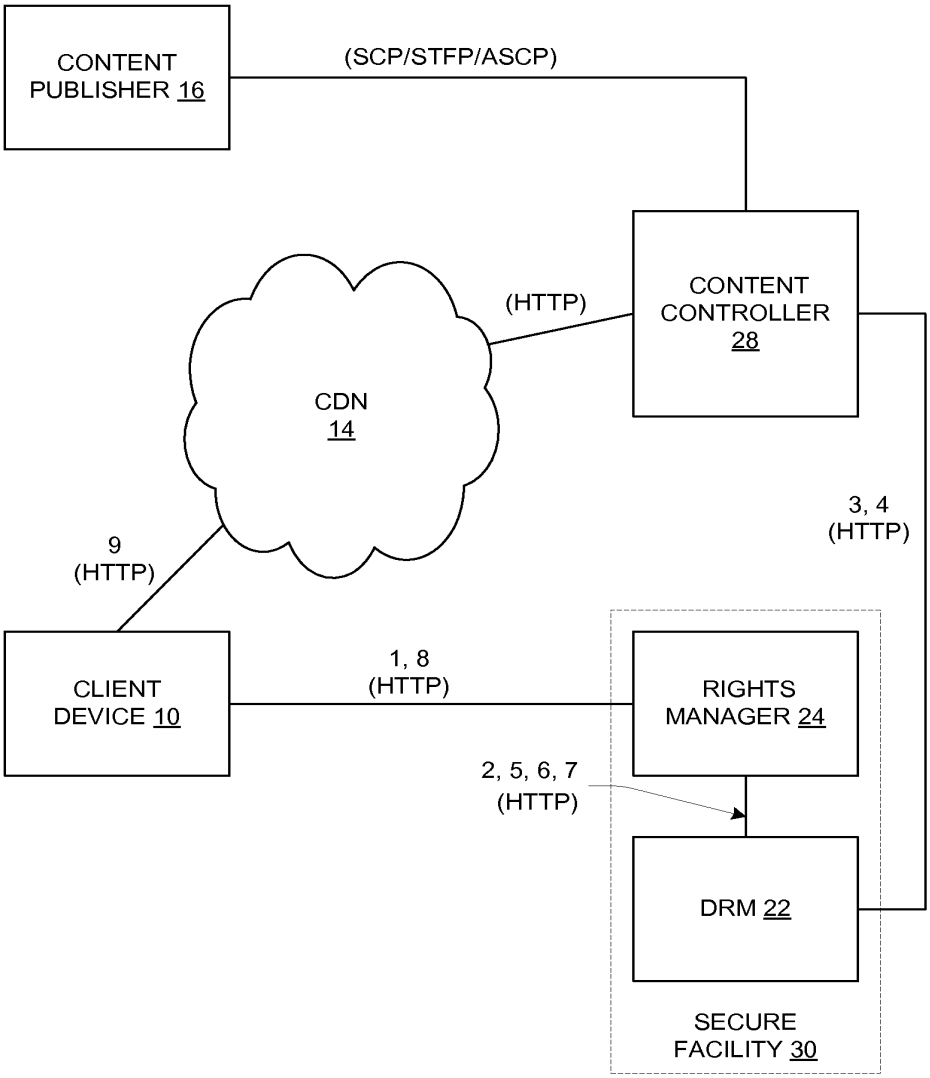

CONTENT PUBLISHER 16
(SCP/STFP/ASCP)
CONTENT CONTROLLER 28
(HTTP)
CDN 14
3, 4 (HTTP)
9 (HTTP)
CLIENT DEVICE 10
1, 8 (HTTP)
RIGHTS MANAGER 24
2, 5, 6, 7 (HTTP)
DRM 22
SECURE FACILITY 30

Fig. 5

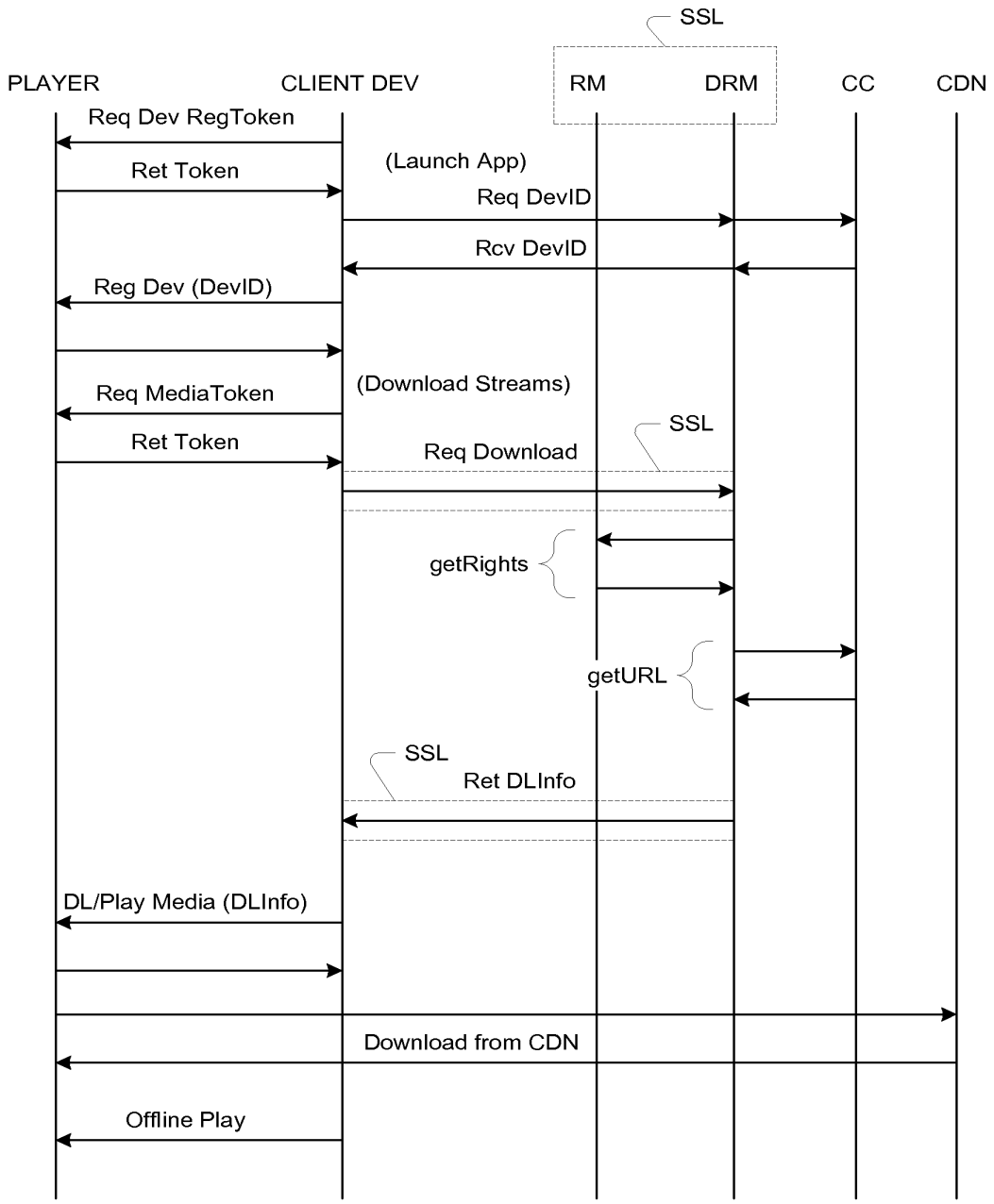

SSL
PLAYER
CLIENT DEV
RM
DRM
CC
CDN
Req Dev RegToken
Ret Token
(Launch App)
Req DevID
Rcv DevID
Reg Dev (DevID)
(Download Streams)
Req MediaToken
SSL
Ret Token
Req Download
getRights
getURL
SSL
Ret DLInfo
DL/Play Media (DLInfo)
Download from CDN
Offline Play

Fig. 6

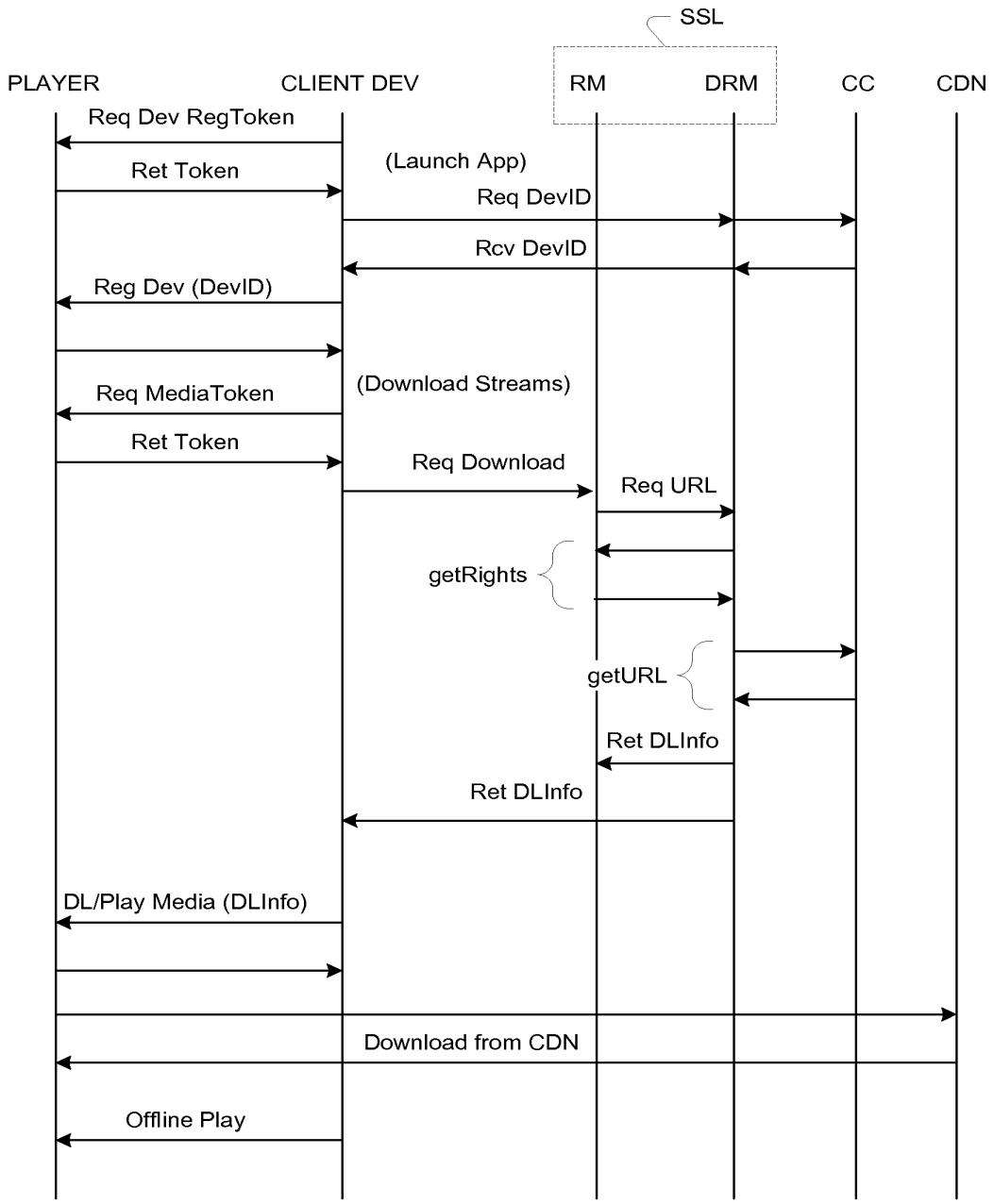

SSL
PLAYER
CLIENT DEV
RM
DRM
CC
CDN
Req Dev RegToken
Ret Token
(Launch App)
Req DevID
Rcv DevID
Reg Dev (DevID)
(Download Streams)
Req MediaToken
Ret Token
Req Download
Req URL
getRights
getURL
Ret DLInfo
Ret DLInfo
DL/Play Media (DLInfo)
Download from CDN
Offline Play

Fig. 7

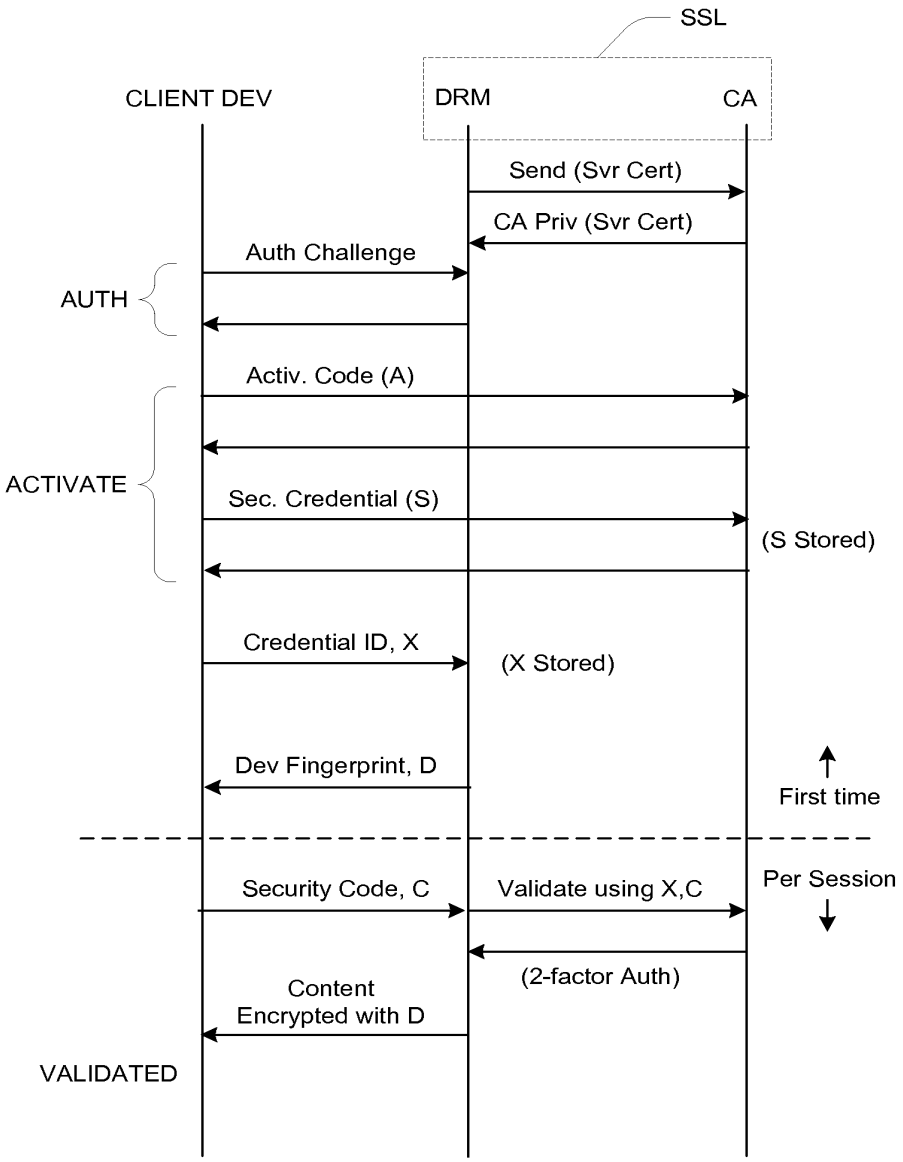

SSL
CLIENT DEV
DRM
CA
Send (Svr Cert)
CA Priv (Svr Cert)
Auth Challenge
AUTH
Activ. Code (A)
ACTIVATE
Sec. Credential (S)
(S Stored)
Credential ID, X
(X Stored)
Dev Fingerprint, D
First time
Security Code, C
Validate using X,C
Per Session
(2-factor Auth)
Content
Encrypted with D
VALIDATED

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 10/45596

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04W 4/00 (2010.01)
USPC - 455/466
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 455/466

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 455/466; 705/50, 51; 713/189 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (PGPB, USPT, USOC, EPAB, JPAB); GoogleScholar
Search Terms: transfer, distribute, file, media, data, protection, security, encryption, mobile, portable, cellular, cellphone, bit rate, streaming, http, hypertext, XOR, exclusive or, switch, change, update, different

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0146122 A1 (Vestergaard et al.) 10 October 2002 (10.10.2002), entire document, especially; abstract, para. [0004], [0023], [0025], [0046], [0062], [0081], [0147], [0171]	1 - 24
Y	US 2006/0212649 A1 (Roberts) 21 September 2006 (20.09.2006), entire document, especially; abstract, para. [0017], [0019], [0021]	1 - 24
Y	US 2005/0240764 A1 (Koshy et al.) 27 October 2005 (27.10.2005), entire document, especially; abstract, para. [0005], [0006], [0015]	10 - 18

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 September 2010 (14.09.2010)	29 SEP 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	KEVIN J. MA
Filer:	James F. Thompson/Sarah Treidel Lamport
Attorney Docket Number:	1082-018.002

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1600**

Electronic Acknowledgement Receipt

EFS ID:	18908964
Application Number:	14266368
International Application Number:	
Confirmation Number:	9269
Title of Invention:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY
First Named Inventor/Applicant Name:	KEVIN J. MA
Customer Number:	47654
Filer:	James F. Thompson/Sarah Treidel Lamport
Filer Authorized By:	James F. Thompson
Attorney Docket Number:	1082-018.002
Receipt Date:	30-APR-2014
Filing Date:	
Time Stamp:	17:34:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1600
RAM confirmation Number	5142
Deposit Account	503661
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		1082-018-002-Application.pdf	94855 546b7a27b22164f51b328133a56c385483f51527	yes	21
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	16	
	Claims		17	20	
	Abstract		21	21	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	1082-018-002-Drawings.pdf	32926 3cad15ebe0f0d5be7cbc1a31da282ec3a2eb3405	no	3
Warnings:					
Information:					
3	Application Data Sheet	1082-018-002-ADS.pdf	1561572 941ef647de3f9d3b581314bf36e13d449012bc1d	no	7
Warnings:					
Information:					
4	Oath or Declaration filed	1082-018-002-Executed-Declarations.PDF	220110 38ba7fac4e02a489aaf7bb48b5553e4fed7ff5c8	no	3
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	1082-018-002-IDS.pdf	612750 cf18ad8841990af8c51b0fa4c046c6767f52f752	no	4
Warnings:					
Information:					
6	Foreign Reference	1082-018-002-WO2010108053.pdf	2371702 87b64486c23411fd3e19403012a5dabd44354a97	no	50
Warnings:					
Information:					
7	Foreign Reference	1082-018-002-WO2011020088.pdf	1125429 9ff6f63ded83fe77e8dee8c2718dbae7eb1cf78e	no	29
Warnings:					

Information:					
8	Non Patent Literature	1082-018-002-draft-pantos-http-live-streaming-06.pdf	1189091 7754e0a2ba1ac3f9f8f9cfaa7ba52d29fcd04183	no	24
Warnings:					
Information:					
9	Non Patent Literature	1082-018-002-Using_Silverlight_with_Windows_Media_DRM-Whitepaper_FINAL.PDF	1143675 ac4bbf5383c624db3984056d8616e9f2dcc82771	no	11
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	32827 174b51cc5f5a514e34f12a2c2594cf0c458bc226	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	8384937	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

TITLE OF APPLICATION

Method and System for Secure Over-the-Top Live Video Delivery

SUMMARY

This invention relates in general to over-the-top (OTT) media delivery and more specifically to encryption key rotation for live streaming media.

As content delivery models move away from streaming distribution over private networks to Web-based delivery of files over the public Internet, referred to as over-the-top (OTT) delivery, traditional content protection paradigms must be modified to support new delivery protocols, e.g., HTTP Live Streaming. For live streaming content with long or indefinite durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised. Traditional key rotation schemes used in private multiple system operator (MSO) and mobile network operator (MNO) distribution networks, where physical security protects the key distribution path, do not extend to use over the public Internet, where communications channels are more susceptible to attack. Furthermore, the encryption used with nascent segment-based HTTP distribution protocols (e.g., HTTP Live Streaming, Silverlight Smooth Streaming, MPEG/3GP Dynamic Adaptive Streaming over HTTP (DASH), etc.) also differs from traditional streaming techniques. Encryption of non-segmented content is typically performed using a single encryption key using a single continuous pass over the content, from start to finish. For segment-based formats, each segment may use the same content encryption key. Though the content encryption key may be salted with a unique initialization vector (IV) for each segment, the IV is not random and provides only limited security.

Methods and apparatus are disclosed for managing the distribution and use of a plurality of content encryption keys for use in the protection of live streaming content. A disclosed method includes generating a series of content encryption keys and providing them serially to a packaging server for encrypting a content item, wherein each content encryption key is provided upon expiration of a period of use of a serially preceding content encryption key. The packaging server generates packaged content for delivery to client devices via a content delivery network, the packaged content including or accompanied by key expiration information usable by the

client devices to identify transitions between sections of the packaged content encrypted by different ones of the content encryption keys. The method further includes providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item. The license server is operative to establish that a requesting client device is authorized to access the content item, and further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established. The transitioning between use of different keys is also referred to herein as key "rotation".

A workflow management system, referred to herein as a workflow manager, is responsible for managing the acquisition of source content from a content management system, preparation of the content, including, but not limited to, transcoding of the content into different encodings (e.g., different bitrates, frame rates, resolutions, sample rates, codecs, etc.), storing the transcoded content in different formats (e.g., 3GP, segmented 3GP, MP4, fragmented MP4, MPEG-TS, segmented MPEG-TS, RTP, etc.), and encrypting the different formats, so that the content is suitable for delivery to a plurality of client devices over a plurality of network infrastructures. The prepared content is then uploaded to a CDN for delivery to clients. Provisions are included for managing when content encryption keys expire, distributing content encryption keys to packaging engines, and distributing content encryption keys to clients.

A client device handles the secure distribution of content by a process including initiating a media playback request and receiving a playback request response, and parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times. The client device retrieves content and manifest files from a content delivery server. During ongoing retrieval of content, the client device detects content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content, issues requests to the license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached, and applies the second key for content decryption after the key rotation boundary is reached.

In the preparation and distribution of content, specifically video content, modern protocols (e.g., HTTP Live Streaming, Silverlight Smooth Streaming, MPEG/3GP Dynamic

Adaptive Streaming over HTTP (DASH), etc.) employ segment-based rate adaptation to deal with fluctuations in bandwidth, whereby segment boundaries provide natural demarcation points for switching bitrates. Another example of a protocol and file format suitable for segment-based rate adaptation is described in PCT Application No. PCT/US2010/027893 filed March 19, 2010, and entitled, Method for Scalable Live Streaming Delivery for Mobile Audiences. Yet another example of a protocol and file format suitable for segment-based rate adaptation is described in PCT Application No. PCT/US2010/028309 filed March 23, 2010, and entitled, Method and System for Efficient Streaming Video Dynamic Rate Adaptation. There are many protocols and methods for generating segmented content, as should be known to those skilled in the art. Any of these segmentation methods are suitable for use in accordance with provisions of the invention. For segment-based formats (e.g., segmented 3GP, fragmented MP4, segmented MPEG-TS, etc.), each segment is independently playable, and therefore needs to be independently encrypted and decryptable. Segments are typically of a fixed duration and, in the case of video content, begin with a key-frame and contain no inter-segment references. Segmentation is performed on each of the different encoding generated by the transcoder, by parsing the resultant encoding and determining segment boundaries. In one embodiment segment boundaries are based on a fixed number of bytes of data. In another embodiment segment boundaries are based on a fixed number of video key frames.

Segments are encrypted on segment boundaries using the current content encryption key and current initialization vector (IV). In one embodiment, the IV may be a simple incrementing integer value. In another embodiment, the IV may be a pseudo-random stream of bits produced by a pseudo-random number generator or stream cipher. Though the IV provides some additional cryptographic strength, it is not random. The generation of new strongly random values for use as content encryption keys and the rotation of content encryption keys provides protection from content encryption keys being compromised in long lived streams. In one embodiment, IVs are reinitialized whenever a content encryption key is rotated. In another embodiment, IVs are not reinitialized when content encryption keys are rotated.

In one embodiment the workflow manager generates content encryption keys with a fixed duration lifespan on a fixed periodic basis. In one embodiment, the content encryption keys may be generated using weak sources of entropy (e.g., processor or wall clock time, /dev/urandom,

etc.). In another embodiment, the content encryption keys may be generated using strong sources of entropy (e.g., hardware sources which rely on electrical static or radioactive decay, /dev/random/, etc.). There are many ways to generate random numbers, as should be known to those skilled in the art. Any method for generating random numbers may be used in accordance with provisions of this method. The workflow manager distributes the content encryption keys and content encryption key lifespan to both a license server and content packaging engine, referred to herein as a packager. The fixed duration lifespan is directly correlated to a fixed period of the live content. The changing of content encryption keys based on the fixed period of the live content is referred to herein as rotation. A history of individual content encryption keys and the order in which they were generated is maintained. Each content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier. In one embodiment, the content encryption key identifiers are selected based on the wall clock time offset from the beginning of the live stream. In another embodiment, the content encryption key identifiers are selected based on a segment number of the prepared content. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The content packaging engine is responsible for encrypting the associated content using the content encryption key. In one embodiment, the packager recognizes the imminent end to the fixed duration lifespan and requests a new content encryption key from the workflow manager. The license server is responsible for distributing content encryption keys to clients. In one embodiment, the license server also distributes fixed duration lifespan information to clients. In one embodiment, when initiating playback of the stream, the client requests the current content encryption key, the next future content encryption key, and the fixed duration lifespan of the keys. The client uses the content encryption keys to decrypt the associated content.

In one embodiment, the workflow manager may initiate content encryption key rotation at any time, outside of the fixed duration lifespan of the existing key. The workflow manager is responsible for notifying the packager of the key rotation request. The packager is responsible for selecting when the new key shall be applied and notifying the workflow manager. In one embodiment, the point at which the key is applied is based on the wall clock time offset from the beginning of the live stream. In another embodiment, the point at which the key is applied is

based on a segment number of the prepared content. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The workflow manager is then responsible for notifying the license server of the new content encryption key, the content encryption key identifier of the new content encryption key, and the lifespan of the new content encryption key. In one embodiment, content encryption key identifiers are selected based on the fixed period of the live content. In one embodiment, the content encryption key identifiers are selected based on the wall clock time offset from the beginning of the live stream. In another embodiment, the content encryption key identifiers are selected based on a segment number of the prepared content. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The packager is responsible for providing in-band notification to the client for the key change. In one embodiment, the notification is embedded in a manifest file that describes the encrypted content. In one embodiment, the manifest may be an m3u8 file. In another embodiment, the manifest may be a Smooth Streaming manifest file. In another embodiment, the manifest may be a DASH MPD file. In another embodiment, the notification is embedded in the segment file name of the encrypted content. In another embodiment, the notification is embedded in a header prepended to the encrypted content. In one embodiment, the header may be a Microsoft PlayReady header. In another embodiment, the header may be an MPEG/3GP DASH header. In another embodiment, the header may be a proprietary segment format header.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages will be apparent from the following description of particular embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of various embodiments of the invention.

Figure 1 is a block diagram of a content delivery system;

Figure 2 is a flow diagram showing content encryption and uploading using content encryption key rotation; and

Figure 3 is a flow diagram showing content downloading and decryption using content encryption key rotation.

DETAILED DESCRIPTION

In the description herein for embodiments of the present invention, numerous specific details are provided, such as examples of components and/or methods, to provide a thorough understanding of embodiments of the present invention. One skilled in the relevant art will recognize, however, that an embodiment of the invention can be practiced without one or more of the specific details, or with other apparatus, systems, assemblies, methods, components, materials, parts, and/or the like. In other instances, well-known structures, materials, or operations are not specifically shown or described in detail to avoid obscuring aspects of embodiments of the present invention.

In this description the term "server" refers to a general-purpose or special-purpose computer, generally including memory, input/output circuitry, and instruction processing logic along with interconnections such as one or more high-speed data buses connecting those components together. Many aspects of the disclosed techniques can be embodied as one or more server computers executing software. Similarly, a "client" herein is a computerized device (also including the above components and executing software) capable of receiving content from a network connection and decoding and rendering the content on a display or similar output device. So-called smartphones are specifically included within the definition of client as used herein.

In Figure 1 is a block diagram of a system 100 for one embodiment of the present invention. As shown, it includes a workflow manager (WFM) 102, one or more packaging servers or “packager(s)” 104, a license server 106, a content delivery network (CDN) 108, client devices or “clients” 110, and a content management system (CMS) 112. Generally in operation, the packager(s) 104 receive source content and process or “package” the source content so that it may be delivered to the clients 110 via the CDN 108. Specifically, the packager(s) 104 perform content encryption using a series of content encryption keys as described below. The CMS 112 provides high-level control over content ingestion, packaging and delivery, while the WFM 102 performs more detailed control operations. The license server 106 is responsible for storing

encryption keys and providing them to the clients 110 for use during playback, as described in more detail below.

The workflow manager (WFM) 102 is responsible for initiating ingestion and preparation of live content. In one embodiment, preparation includes transcoding audio and video into a plurality of encodings using different codecs, bitrates, frame rates, sample rates, and resolutions. The transcoded content is then written into a plurality of output files. In one embodiment, a plurality of output files contain the same transcoded content encapsulated in different container formats (e.g., 3GP, MP4, MPEG-TS, WMV, MOV, etc.). In one embodiment, the prepared output files are segmented into fixed duration segment files (e.g., MPEG-TS segments, fragmented MP4 segments, 3GP DASH segments, etc.). In one embodiment, the output files, both segmented and un-segmented, are encrypted using standard encryption protocols (e.g., AES-128, HC-128, RC4, etc.). In one embodiment, IVs for the encryption protocol are reinitialized by the packager 104 whenever a content encryption key is rotated. In another embodiment, IVs for the encryption protocol are not reinitialized when content encryption keys are rotated. In one embodiment, all preparation steps are performed by a single content packaging server or packager 104. In another embodiment, individual preparation steps (e.g., transcoding, segmentation, encryption, etc.) may be performed across different physical packaging servers 104. The packager 104 which performs encryption acquires content encryption keys from the workflow manger 102. In one embodiment the WFM 102 and packager 104 reside in the same physical server. In another embodiment, the WFM 102 and packager 104 reside in different physical servers in the same data center. In another embodiment, the WFM 102 and packager 104 reside in different physical servers in remote data centers.

The WFM 102 receives an ingestion request from the content management system (CMS) 112. The request specifies a security profile. In one embodiment, the security profile includes content encryption information, including cipher specification and content encryption key expiration policies. The WFM 102 generates an initial content encryption key and assigns it a content encryption key identifier. In one embodiment, the content encryption key identifier is initially set to zero and all future content encryption key identifiers are based on a relative offset to the initial content encryption key identifier. In one embodiment, the content encryption key identifiers are based off a next sequential integer value, offset from the previous content

encryption key identifier. In another embodiment, the content encryption key identifiers are based off the wall clock time offset from the time the initial content encryption key identifier was generated. In another embodiment, the content encryption key identifiers are based off of segment numbers, as produced by the packager 104 during segmentation. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames.

The WFM 102 then initiates content preparation by assigning a packager 104 to begin acquiring the source content and performing transcoding and segmentation as required. The WFM 102 provides the initial content encryption key and lifespan of the key to the packager 104 responsible for encryption of the prepared outputs. The packager 104 encrypts the content using the initial content encryption key until it expires. In one embodiment, the expiration time is based on a relative wall clock time offset to the time preparation was started. In another embodiment, the content encryption key identifiers are based off of segment numbers, as produced by the packager 104 during segmentation. Segmentation detects segment boundaries and assigns a fixed amount of data to each individual segment. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video "key frames" (e.g., I-Frames in MPEG encoding). In one embodiment, before the content encryption key expires, the packager 104 requests a new key from the WFM 102. In one embodiment, the new content encryption key has the same lifespan as the previous content encryption key. The new content encryption key is made available by the WFM 102 to the packager 104 before the previous content encryption key has expired to allow for uninterrupted encryption. In one embodiment, if the packager 104 is unable to obtain a new content encryption key from the WFM 102 prior to the expiration of the current content encryption key, the packager 104 will continue to use the current content encryption key until such time as it is able to obtain a new key from the WFM 102.

Encrypted content is uploaded by the packager 104 to a content delivery network (CDN) 108, from which it may be retrieved by clients 110. In one embodiment, manifest files are also uploaded by the packager 104 to the CDN 108. The clients 110 must first obtain the content encryption keys from the license server 106, before they may decrypt and render encrypted content. In one embodiment, clients 110 retrieve content encryption keys using HTTPS.

Generally, the license server 106 is responsible for ensuring that a client device 110 is authorized to access any protected content before providing the encryption keys for such content to a requesting client110. In one embodiment, clients 110 are verified by the license server 106 using client certificate verification. In another embodiment, clients 110 are verified using login credentials. The license server 106 is notified of new content encryption keys by the WFM 102 as they are generated. In one embodiment, the license server 106 stores the content encryption key, content encryption key identifier, content encryption key lifespan (or expiration), and the location of the encrypted content. In one embodiment, the information is stored as an encrypted token in a database. In one embodiment the WFM 102 and license server 106 reside in the same physical server. In another embodiment, the WFM 102 and license server 106 reside in different physical servers in the same data center. In another embodiment, the WFM 102 and license server 106 reside in different physical servers in different data centers. In one embodiment, the license server 106 registers client devices 110 and verifies the right of each client device 110 to view the content. If the client 110 has the right to view the content, the license server 106 provides the content encryption key, content encryption key lifespan (or expiration), and the location of the encrypted content.

In one embodiment, the WFM 102 may issue a new unsolicited content encryption key to the packager 104. In one embodiment, the WFM 102 pushes the new content encryption key to the packager 104 when the current content encryption key is nearing the end of its lifespan. In one embodiment, the new content encryption key is pushed ahead of the current content key expiration, and the packager 104 waits until the current content encryption key has expired before applying the new content encryption key. In another embodiment, the new content encryption key is pushed ahead of the current content key expiration with explicit instructions to apply the key as soon as possible, in which case the packager 104 does not wait until the current content encryption key has expired before applying the new content encryption key.

In one embodiment, the WFM 102 pushes the new content encryption key to the packager 104 when the current content encryption key is deemed to be no longer secure (e.g., if the content encryption key has been compromised). The packager 104 waits until the next available encryption boundary before applying the new content encryption key, and then notifies the WFM 102 of the exact boundary at which it expired the previous content encryption key. In

one embodiment, the encryption boundary is a segment boundary. In one embodiment the segment boundaries are based on a fixed number of bytes of data. In another embodiment the segment boundaries are based on a fixed number of video key frames. The lifespan of the new content encryption key may be aligned to the periodic use period boundaries of the previous content encryption keys. In one embodiment, the expiration of the new content encryption key is set to the expiration time of the previous content encryption key. Thus if the new content encryption key was applied when the previous content encryption key had 10 minutes left in its lifespan, for example, then the lifespan of the new content encryption key is set to 10 minutes. In another embodiment, the expiration of the new content encryption key is set to the next periodic expiration time which is greater than half the fixed expiration period duration. Thus, if the lifespan of content encryption keys is 60 minutes and the previous content encryption key had 10 minutes left in its lifespan, for example, then the lifespan of the new content encryption key is set to 70 minutes (10 + 60) because the remaining time of 10 minutes is less than half the fixed expiration period duration (60 / 2 = 30).

In one embodiment, the packager 104 notifies the client 110 of a key change by prepending a header to the encrypted content which contains a flag that describes the expiration of the previous key. In one embodiment, the header may be a Microsoft PlayReady header. In another embodiment, the header may be an MPEG/3GP DASH header. In another embodiment, the header may be a proprietary segment format header. In another embodiment, the packager 104 notifies the client 110 of the key change by updating a manifest file that describes the encrypted content with a flag that describes the expiration of the previous key. In one embodiment, the manifest may be an m3u8 file. In another embodiment, the manifest may be a Smooth Streaming manifest file. In another embodiment, the manifest may be a DASH MPD file. In another embodiment, the packager 104 notifies the client 110 of the key change in the file name of the encrypted content by appending a flag that describes the expiration of the previous key.

Figure 2 is a flow chart 200 describing a process for obtaining and rotating content encryption keys in a packager 104. In step 202, the WFM 102 receives an ingestion request from a CMS 112. In one embodiment, the request is an HTTP POST of XML data containing information including, but not limited to, transcode parameters, segmentation parameters,

encryption parameters, source content location, and CDN parameters. In one embodiment, the WFM 102 may have predefined profiles for media preparation, content encryption, and CDN upload which are referenced in the ingestion request. In one embodiment the encryption parameters include a fixed period duration for key rotation.

It should be noted that the fixed period duration for key rotation may be viewed as a "target" period, as the packager 104 may not expire a key on the exact boundary. Generally, the packager 104 will not expire a key earlier than the end of a target period.

In step 204, the WFM 102 instructs the packager 104 to begin preparation of the content. A packager 104 begins acquiring the source content, transcoding the source content and segmenting the source content. As each segment is produced, it is delivered to the packager 104 responsible for encrypting the prepared content.

In step 205, the packager 104 responsible for encryption waits for new segments to become available. Once a new segment becomes available, processing proceeds to step 206 where this packager 104 checks to see if a new content encryption key has been received from the WFM 102. The content encryption key may be an initial content encryption key provided by the WFM 102 with the initial content preparation request. The content encryption key may be received in response to a content encryption key request from the packager 104 (originating from step 218). The content encryption key may be received via a proactive push from the WFM 102 in anticipation of a periodic content encryption key expiration event. The content encryption key may be an unsolicited content encryption key pushed by the WFM 102 as a security precaution necessitated by security policies (e.g., the current content encryption key was compromised or the current content encryption was found to be not sufficiently random).

If a new content encryption key was received, processing proceeds to step 208 where the expiration times for the current content encryption key and the new content encryption key are determined. If the new content encryption key is an initial content encryption key or a regularly scheduled update in advance of a periodic content encryption key expiration (either requested by the packager 104, or pushed proactively by the WFM 102), the lifespan is set to the fixed period duration. If the new content encryption key is not a regularly scheduled update and must be applied as soon as possible, the expiration of the current content encryption key and the new content encryption key are calculated. In one embodiment, the new content encryption key is

applied at the next segment boundary. In one embodiment, the lifespan of the new content encryption key is set to the remainder of the lifespan of the current content encryption key. In another embodiment, the lifespan of the new content encryption key is rounded up to the remainder of the lifespan of the current content encryption key plus one fixed key rotation period duration. Once the content encryption key expirations have been set, processing proceeds to step 210.

In step 210, executed after step 208 or after step 206 when no new content encryption key is received, the packager 104 checks the expiration of current content key to see if a new key should be applied. If the current content encryption key has not yet expired or if a replacement content encryption key has not yet been obtained, processing proceeds to step 214. If the current content encryption key needs to be expired and a replacement content encryption key is available, processing proceeds to step 212 where the current content encryption key is expired and replaced with the pending content encryption key. The key expiration time from the WFM 102 may be viewed as a "suggested" expiration time, as the packager 104 may not be able to expire the key at the exact specified time. In one embodiment, the packager 104 notifies the WFM 102 of the exact time (segment number) at which a new key took effect (i.e., began to be used to encrypt content segments). In this case, the WFM 102 may wait to push the new key to the license server 106 only after receiving confirmation from the packager 104 that the new key has taken effect. In one embodiment, the IV is reinitialized when the content encryption key is expired. In another embodiment, when content encryption key is expired, the packager 104 continues to use the existing IV stream. Once the new content encryption key is in place, processing proceeds to step 214. In step 214, the segment received in step 205 is encrypted using the current content encryption key and the cipher specified in the ingestion request. Once the segment has been encrypted it is uploaded to the CDN 108 and processing proceeds to step 216.

In step 216, the packager 104 checks to see if the current content encryption key is going to expire in the near future. In one embodiment, when the current content encryption key is about to expire, the packager 104 proactively requests a new content encryption key ahead of time to prevent any interruption of encryption services. If the current content encryption key is not close to expiring, processing proceeds back to step 205 where the packager 104 waits for the

next segment which needs to be encrypted. If the current content encryption key is within a fixed threshold of expiring, processing proceeds to step 218 where the packager 104 requests a new content encryption key from the WFM 102. In one embodiment, the threshold is set as a fixed amount of wall clock time before the current content encryption key will expire (e.g., 1 minute prior to the expiration of the current content encryption key). In another embodiment, the threshold is set as a fixed number of segments before the current content encryption key will expire (e.g., 6 segments before the expiration of the current content encryption key, where 10 second fixed duration segments would yield a threshold of approximately 1 minute). In another embodiment, the threshold is set as a fixed percentage of the fixed period content encryption key lifespan (e.g., when the lifespan of the current content encryption key is 90% complete). Once the request for a new content encryption key has been sent in step 218, processing proceeds back to step 205 where the packager 104 waits for the next segment which needs to be encrypted.

Figure 3 is a flow chart 300 describing a process for detecting the rotation of content encryption keys and retrieving updated content encryption keys. In step 302, the client 110 issues a playback request to the WFM 102. In one embodiment, the initial playback request may require registration of the client 110, user login, or some other authentication mechanism. In step 304, the client 110 retrieves and parses the content information, including content formats, content bitrates, content locations, content encryption keys, and content encryption key expiration. In one embodiment, the WFM 102 and license server 106 are deployed on the same physical machine with the ability to function through a single software interface when dealing with the client 110, and the WFM 102 may return all the necessary information, including content formats, content bitrates, content locations, content encryption keys, and content encryption key expiration, to the client 110. In another embodiment, the WFM 102 and license server 106 are deployed separately, and the client 110 must make a first request to the WFM 102 to retrieve content formats, content bitrates, content locations, and the license server 106 location. The client 110 then makes a second request to the license server 106 to retrieve content encryption keys and content encryption key expiration information.

In one embodiment, the retrieval of content encryption keys is performed over a secure channel. In one embodiment, the channel is secured using HTTPS. In another embodiment, the channel could be secured with a proprietary encryption mechanism. There are numerous ways to

secure a communications channel, as should be known to those skilled in the art. Any method for securing a communications channel may be applied in step 304. In one embodiment, the channel requires authentication of the client device 110. In one embodiment, authentication is performed using SSL client authentication. In another embodiment, authentication is performed using proprietary certificate validation procedures. In another embodiment, authentication is performed using symmetric key encryption using white-box encryption methods. In another embodiment, user login credentials are passed over the secure channel. There are numerous ways to authenticate a client device 110, as should be known to those skilled in the art. Any method for authenticating a client device 110 may be applied in step 304. Once the initial playback response message processing has completed, processing proceeds to step 306.

In step 306, the client 110 retrieves the next available segment from the CDN 108. In one embodiment, the first available segment is specified by the WFM 102 in the initial playback response message. In another embodiment, the first available segment is specified in a manifest file retrieved from the CDN 108. In one embodiment, subsequent segments are identified based on sequential segment numbering using a well-known file naming scheme. In another embodiment, subsequent segments are identified by a manifest file in the CDN 108. In another embodiment, subsequent segments are identified based on the relative wall clock time in which they are generated, by performing directory listings or using a watched directory to determine when new segments become available.

Once the new segment is retrieved, processing proceeds to step 308 where the client 110 checks to see if a key change is signaled, i.e., a key change was requested outside of any fixed duration lifespan. This can occur for security reasons as mentioned above. In one embodiment, the packager 104 notifies the client 110 of the key change by prepending a header to the encrypted content which contains a flag that describes the expiration of the previous content encryption key and the content encryption key identifier of the new content encryption key to be applied. In one embodiment, the header may be a Microsoft PlayReady header. In another embodiment, the header may be an MPEG/3GP DASH header. In another embodiment, the header may be a proprietary segment format header. In another embodiment, the packager 104 notifies the client 110 of the key change by updating a manifest file that describes the encrypted content with a flag that describes the expiration of the previous content encryption key and the

content encryption key identifier of the new content encryption key to be applied. In one embodiment, the manifest may be an m3u8 file. In another embodiment, the manifest may be a Smooth Streaming manifest file. In another embodiment, the manifest may be a DASH MPD file. In another embodiment, the packager 104 notifies the client 110 of the key change in the file name of the encrypted content by appending a flag that describes the expiration of the previous content encryption key and the content encryption key identifier of the new content encryption key to be applied. If a content encryption key change request is detected, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used. The client 110 then proceeds to step 310.

In step 310, the client 110 checks the expiration of current content key to see if a new key should be applied. There are two cases – normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted. If the current content encryption key has not yet expired, processing proceeds to step 314. If the current content encryption key needs to be expired, processing proceeds to step 312 where the key is "rotated", i.e., the current content encryption key is expired and a new one is put into use. The client 110 first checks whether the content encryption key corresponding to a key change notification in step 308 has already been retrieved by prefetching as described below with reference to step 318. If the new content encryption key has already been retrieved, the current content encryption key is replaced with that pending content encryption key. If the new content encryption key has not been retrieved yet (e.g., due to early expiration of the current content encryption key for security reasons, or content encryption key retrieval failures in step 318), the client 110 must issue a new content encryption key request to the license server 106 to retrieve the new content encryption key, then replace the current content encryption key with the newly retrieved content encryption key.

In one embodiment, the encryption algorithm initialization vector (IV) is reinitialized when the content encryption key is expired. In another embodiment, when content encryption key is expired, the client 110 continues to use the existing IV stream.

Once the new content encryption key is in place, processing proceeds to step 314. In step 314, the segment retrieved in step 306 is decrypted using the current content encryption key and

the cipher specified in the initial playback response message. Once the segment has been decrypted it is passed to the media player for rendering and processing proceeds to step 316.

In step 316, the client 110 checks to see if the current content encryption key is going to expire in the near future or if a content encryption key change request for a future segment was detected in step 308. In one embodiment, when the current content encryption key is about to expire, the client 110 proactively requests a new content encryption key ahead of time to prevent any latency in or interruption of decryption services. If the current content encryption key is not close to expiring and a content encryption key change request was not detected in step 308, processing proceeds back to step 306 where the client 110 begins retrieving the next segment. If the current content encryption key is within a fixed threshold of expiring or a content encryption key change request was detected in step 308, processing proceeds to step 318 where the client 110 requests a new content encryption key from the license server 106. In one embodiment, the threshold is set as a fixed amount of wall clock time before the current content encryption key will expire. In another embodiment, the threshold is set as a fixed number of segments before the current content encryption key will expire. In another embodiment, the threshold is set as a fixed percentage of the fixed period content encryption key lifespan. Once the request for a new content encryption key has been sent in step 318, processing proceeds back to step 306 where the client 110 begins retrieving the next segment.

While various embodiments of the invention have been particularly shown and described, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention as defined by the appended claims.

CLAIMS

What is claimed is:

1. A method for handling secure distribution of content comprising:

initiating a media playback request and receiving a playback request response;

parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;

retrieving content and manifest files from a content delivery server;

detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

issuing requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and

applying the second key for content decryption after the key rotation boundary is reached.

2. The method of claim 1, wherein the content encryption keys and content encryption key identifiers returned in the playback request response include the content encryption key and associated identifier currently being applied as well as a future content encryption key and associated identifier yet to be applied.

3. The method of claim 1, wherein the content encryption key expiration returned in the playback request response is expressed as an expected minimum interval between periodic key rotation.

4. The method of claim 3, further comprising: timing the prefetching of a next un-retrieved content encryption key based on an expected expiration of the content encryption key currently being used.

5. The method of claim 4, further comprising: prefetching a next un-retrieved key a fixed duration before the expected expiration of the content encryption key currently being used.

6. The method of claim 4, further comprising: prefetching a next un-retrieved key within a period of time after the expected expiration of the content encryption key currently being applied, the period of time beginning at the expected expiration of the content encryption key currently being used, and ending at a duration calculated as a fixed percentage of a fixed periodic content encryption key expiration interval.

7. The method of claim 1, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

8. The method of claim 7, further comprising: the identifier being calculated as monotonically increasing sequential integer values based on the number of segments or video frames generated during a fixed periodic content encryption key expiration interval.

9. The method of claim 7, further comprising: the identifier being calculated as an expected wall clock time for applying the next content encryption key based on a fixed periodic content encryption key expiration interval.

10. The method of claim 1, wherein license server communications are secured and authenticated using a selected one of Secure Sockets Layer and a token-based technique using a token encrypted with a symmetric key.

11. The method of claim 10, wherein the token-based technique employs white box encryption to encrypt the token.

12. The method of claim 1, wherein actual content encryption key rotation boundaries are detected based on real-time in-band notifications.

13. The method of claim 12, wherein content encryption key rotation boundaries are detected based on notifications in an unencrypted header portion of the encrypted content files.

14. The method of claim 12, wherein content encryption key rotation boundaries are detected based on notifications present in the content manifest file, the content manifest file being selected from an m3u8 file, an IIS Smooth Streaming manifest file, a DASH MPD file and a proprietary manifest file.

15. The method of claim 12, wherein content encryption key rotation boundaries are detected based on a notification embedded in the file name of the encrypted content file.

16. A computerized device operable as a client for handling secure distribution of content, comprising:

memory operative to store computer program instructions;

one or more processors;

input/output interface circuitry; and

interconnect circuitry coupling the memory, processors and input/output interface circuitry together,

wherein the processors are operative to execute the computer program instructions from the memory to cause the computerized device to:

initiate a media playback request and receive a playback request response;

parse content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;

retrieve content and manifest files from a content delivery server;

detect content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

issue requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and

apply the second key for content decryption after the key rotation boundary is reached.

17. The computerized device of claim 16, wherein the content encryption keys and content encryption key identifiers returned in the playback request response include the content encryption key and associated identifier currently being applied as well as a future content encryption key and associated identifier yet to be applied.

18. The computerized device of claim 17, wherein the computer program instructions further cause the computerized device to time the prefetching of a next un-retrieved content encryption key based on an expected expiration of the content encryption key currently being used.

19. The computerized device of claim 16, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

20. The computerized device of claim 16, wherein actual content encryption key rotation boundaries are detected based on real-time in-band notifications.

ABSTRACT

A method is provided for managing key rotation (use of series of keys) and secure key distribution in over-the-top content delivery. The method provided supports supplying a first content encryption key to a content packaging engine for encryption of a first portion of a video stream. Once the first content encryption key has expired, a second content encryption key is provided to the content packaging engine for encryption of a second portion of a video stream. The method further provides for notification of client devices of imminent key changes, as well as support for secure retrieval of new keys by client devices. A system is also specified for implementing a client and server infrastructure in accordance with the provisions of the method.

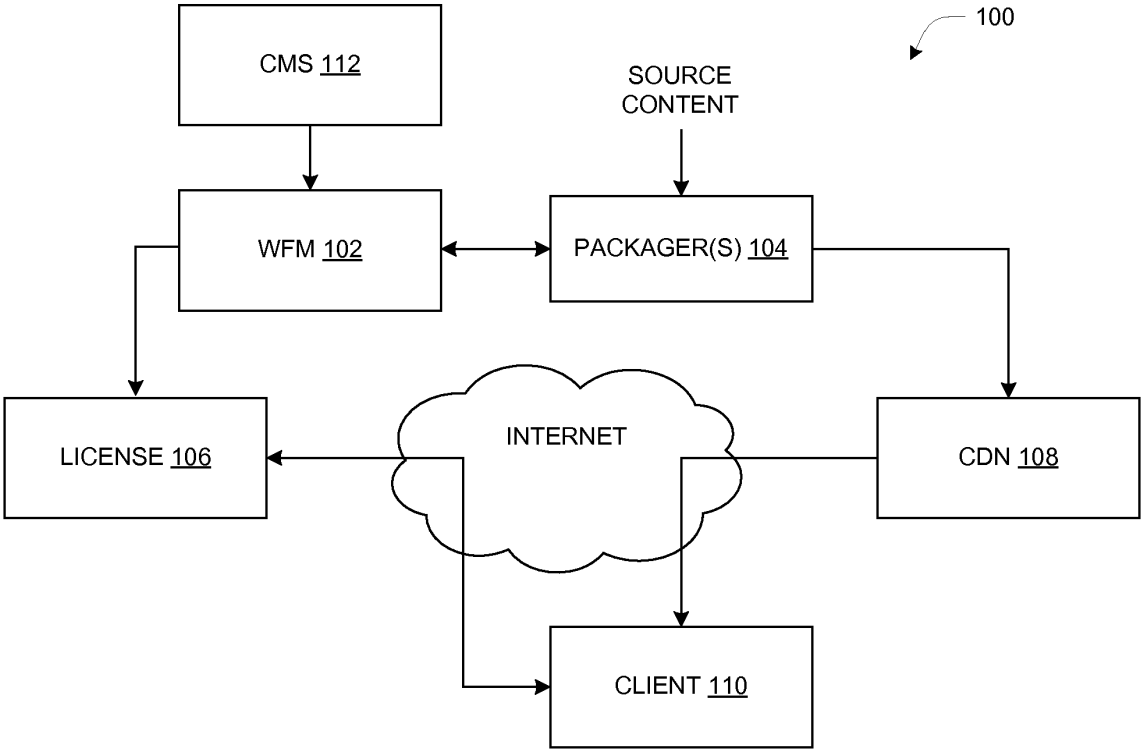

100
CMS 112
SOURCE CONTENT
WFM 102
PACKAGER(S) 104
LICENSE 106
INTERNET
CDN 108
CLIENT 110

Fig. 1

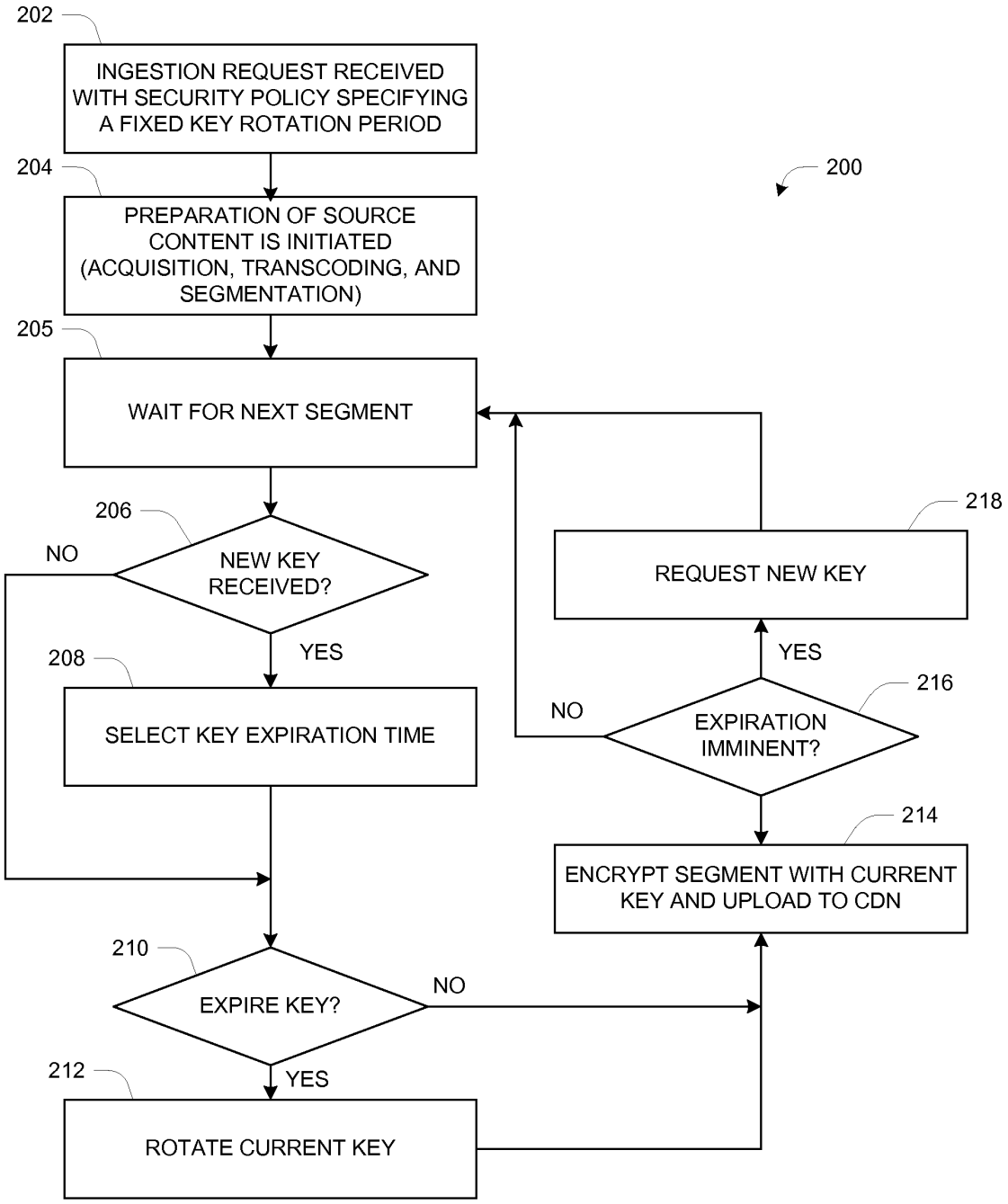

202
INGESTION REQUEST RECEIVED WITH SECURITY POLICY SPECIFYING A FIXED KEY ROTATION PERIOD
204
PREPARATION OF SOURCE CONTENT IS INITIATED (ACQUISITION, TRANSCODING, AND SEGMENTATION)
200
205
WAIT FOR NEXT SEGMENT
206
NEW KEY RECEIVED?
NO
YES
208
SELECT KEY EXPIRATION TIME
218
REQUEST NEW KEY
YES
216
NO
EXPIRATION IMMINENT?
214
ENCRYPT SEGMENT WITH CURRENT KEY AND UPLOAD TO CDN
210
EXPIRE KEY?
NO
212
YES
ROTATE CURRENT KEY

Fig. 2

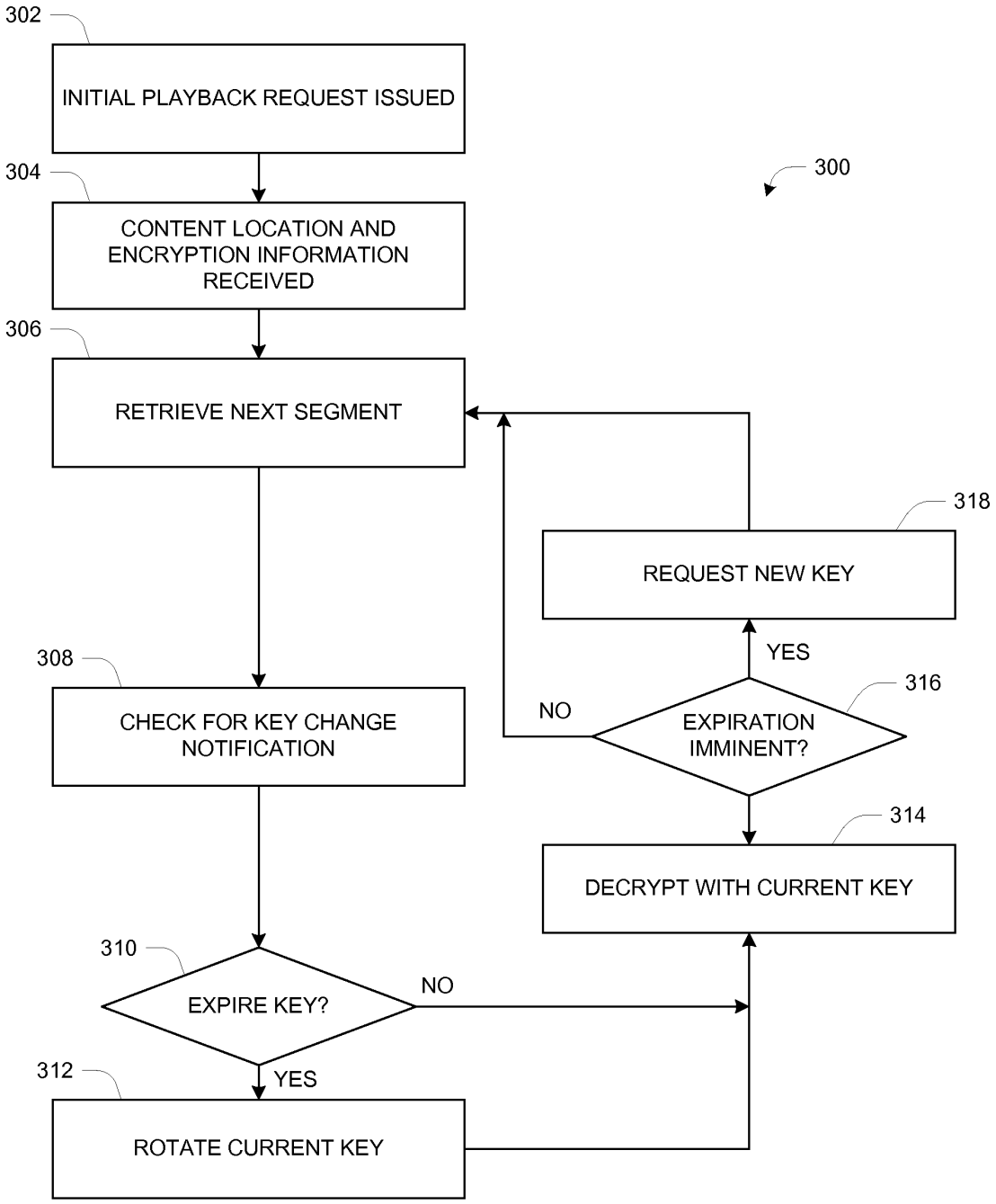

302
INITIAL PLAYBACK REQUEST ISSUED
304
CONTENT LOCATION AND ENCRYPTION INFORMATION RECEIVED
300
306
RETRIEVE NEXT SEGMENT
318
REQUEST NEW KEY
YES
308
316
NO
CHECK FOR KEY CHANGE NOTIFICATION
EXPIRATION IMMINENT?
314
DECRYPT WITH CURRENT KEY
310
NO
EXPIRE KEY?
312
YES
ROTATE CURRENT KEY

Fig. 3

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1082-018.002
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Kevin	J.	Ma	

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

City	Nashua	State/Province	NH	Country of Residence i	US

Mailing Address of Inventor:

Address 1	16 Bicentennial Drive		
Address 2			
City	Nashua	State/Province	NH
Postal Code	03062	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Robert		Hickey	

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

City	Bedford	State/Province	MA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	2 Fawn Circle		
Address 2			
City	Bedford	State/Province	MA
Postal Code	01730	Country i	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Paul		Tweedale	

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1082-018.002
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

City	Andover	**State/Province**	MA	**Country of Residence** i	US

Mailing Address of Inventor:

Address 1	150 Shawsheen Road		
Address 2			
City	Andover	**State/Province**	MA
Postal Code	01810	**Country** i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	47654		
Email Address	docket@bainwoodhuang.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY		
Attorney Docket Number	1082-018.002	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	3	**Suggested Figure for Publication (if any)**	3

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country i

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1082-018.002
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	(•) Customer Number	( ) US Patent Practitioner	( ) Limited Recognition (37 CFR 11.9)
Customer Number	47654		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13530997	2012-06-22
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13530997	Claims benefit of provisional	61500316	2011-06-23
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.			Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1082-018.002
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1082-018.002
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

- (●) Assignee
- ( ) Legal Representative under 35 U.S.C. 117
- ( ) Joint Inventor
- ( ) Person to whom the inventor is obligated to assign.
- ( ) Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. [X]

Organization Name	Azuki Systems, Inc.		
Mailing Address Information:			
Address 1	43 Nagog Road		
Address 2	Suite 105		
City	Acton	**State/Province**	MA
Country i	US	Postal Code	01720
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. [ ]

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	1082-018.002
	Application Number	
Title of Invention	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/James F. Thompson/			Date (YYYY-MM-DD)	2014-04-30
First Name	James F.	Last Name	Thompson, Esq.	Registration Number	36699

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

This declaration is directed to an application entitled

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

which is further identified by Attorney Docket Number 1082-018.002.

As the below named inventor, I hereby declare that:

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

I hereby acknowledge that a person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the United States Patent and Trademark Office all information known to the person to be material to patentability as defined in § 1.56.

LEGAL NAME OF INVENTOR

Inventor: Kevin J. Ma Date (Optional): 4/29/14

Signature: _____

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

This declaration is directed to an application entitled

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

which is further identified by Attorney Docket Number 1082-018.002.

As the below named inventor, I hereby declare that:

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

I hereby acknowledge that a person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the United States Patent and Trademark Office all information known to the person to be material to patentability as defined in § 1.56.

LEGAL NAME OF INVENTOR

Inventor: Robert Hickey Date (Optional): 4/29/14

Signature: _____

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

This declaration is directed to an application entitled

METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY

which is further identified by Attorney Docket Number 1082-018.002.

As the below named inventor, I hereby declare that:

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

I hereby acknowledge that a person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the United States Patent and Trademark Office all information known to the person to be material to patentability as defined in § 1.56.

LEGAL NAME OF INVENTOR

Inventor: Paul Tweedale Date (Optional): 4/29/14

Signature: _____